BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT COOPERATION TREATY 10/069795

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING THE FILING OF AMENDMENTS OF THE CLAIMS

(PCT Administrative Instructions, Section 417)

To:

OGASAWARA, Shiro
Daisan-Longev'Bldg., 3-11, Enokicho
Suita-shi, Osaka 564-0053
JAPON

Date of mailing (day/month/year) 06 December 2001 (06.12.01)	
Applicant's or agent's file reference PCT01-052	**IMPORTANT NOTIFICATION**
International application No. PCT/JP01/05484	**International filing date** (day/month/year) 27 June 2001 (27.06.01)
Applicant MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. et al	

1. The applicant is hereby notified that amendments to the claims under Article 19 were received by the International Bureau on:

   26 November 2001 (26.11.01)

2. This date is within the time limit under Rule 46.1.

   Consequently, the international publication of the international application will contain the amended claims according to Rule 48.2(f), (h) and (i).

3. The applicant is reminded that the international application (description, claims and drawings) may be amended during the international preliminary examination under Chapter II, according to Article 34, and in any case, before each of the designated Offices, according to Article 28 and Rule 52, or before each of the elected Offices, according to Article 41 and Rule 78.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

Authorised officer

Shinji IGARASHI
Telephone No.: (41-22) 338.83.38

ATTACHMENT D

PATENT COOPERATION TREATY

10/069795

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
OGASAWARA, Shiro
Daisan-Longev'Bldg., 3-11, Enokicho
Suita-shi, Osaka 564-0053
JAPON

受領
'02.1.15
小笠原

Date of mailing (day/month/year)	
03 January 2002 (03.01.02)	
Applicant's or agent's file reference	IMPORTANT NOTICE
PCT01-052	

International application No.	International filing date (day/month/year)	Priority date (day/month/year)
PCT/JP01/05484	27 June 2001 (27.06.01)	29 June 2000 (29.06.00)

Applicant
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. et al

1. Notice is hereby given that the International Bureau has **communicated**, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this notice:
   KR,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   CN

   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this notice is a copy of the international application as published by the International Bureau on
   03 January 2002 (03.01.02) under No. WO 02/01790

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, **a demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination (at present, all PCT Contracting States are bound by Chapter II).

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and the PCT Applicant's Guide, Volume II.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
J. Zahra

Telephone No. (41-22) 338.91.11

ATTACHMENT A

10/069795

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05484

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/00, G11B20/10, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/00, G11B20/10, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, JICST FILE on Science and Technology content, key, encryption, DVD

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 00/22539 A1 (Sony Corporation), 20 April, 2000 (20.04.00), page 100, lines 8 to 15; page 101, lines 1 to 4; page 122, line 12 to page 123, line 3 & JP 2000-123084 A & JP 2000-124890 A & JP 2000-138673 A & JP 2000-188595 A & AU 9961231 A & EP 1039392 A1 & CN 1289421 A	1,4,8,10 2,3,5,9
Y	JP 10-293724 A (Toshiba Corporation), 04 November, 1998 (04.11.98), Par. Nos. [0039] to [0076] (Family: none)	2,3,5,9
A	JP 11-39794 A (Matsushita Electric Ind. Co., Ltd.), 12 February, 1999 (12.02.99), Full text (Family: none)	1-5,8-10
A	JP 2000-122539 A (Matsushita Electric Ind. Co., Ltd.), 28 April, 2000 (28.04.00), Par. Nos. [0018], [0044], [0045] (Family: none)	1-5,8-10

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 September, 2001 (11.09.01)	25 September, 2001 (25.09.01)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05484

B x I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

B x II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The examiner has judged that the inventions of claims of the international application are divided into eight groups. However, according to the decision on the protest against the additional fee, the inventions are divided into seven groups.

1. The inventions of claims 1-5, 8-10
2. The inventions of claims 6, 7, 11, 12
3. The inventions of claims 13, 14
4. The inventions of claims 15, 16
5. The invention of claim 17
6. The invention of claim 18
7. The invention of claim 19

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☒ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

Claims 1 to 5, 8 to 10

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☒ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05484

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Supervision: Shin ICHIMATSU, "Data Hogo to Angou-ka no Kenkyuu; Computer Network no Anzensei", Nippon Keizai Shinbunsha, 29 July, 1983 (29.07.83), pages 201 to 206 (especially, page 204, 3 Data Angou Kagi no Touroku)	1-5,8-10

国際調査報[redacted]　　国際出願番号[redacted]CT／JP01／05484

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／00, G11B20／10, G06F15／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／00, G11B20／10, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI，JICST科学技術文献データベース　content, key, encryption, DVD

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	WO 00/22539 A1（ソニー株式会社） 20. 4月.2000(20.04.00)，第100頁第8-15行，第101頁第1-4行， 第122頁第12行－第123頁第3行 & JP 2000-123084 A & JP 2000-124890 A & JP 2000-138673 A & JP 2000-188595 A & AU 9961231 A & EP 1039392 A1 & CN 1289421 A	1, 4, 8, 10
Y		2, 3, 5, 9
Y	JP 10-293724 A（株式会社東芝） 4.11月.1998(04.11.98)，第39-76段落（ファミリなし）	2, 3, 5, 9
A	JP 11-39794 A（松下電器産業株式会社） 12. 2月.1999(12.02.99)，全頁を参照（ファミリなし）	1-5, 8-10

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 11. 09. 01	国際調査報告の発送日　25.09.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里　裕正　　5M　9364 電話番号　03－3581－1101　内線　3597

様式PCT／ISA／210（第2ページ）（1998年7月）

国際[redacted]査報告

国際[redacted]番号　PCT／JP01／05484

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

審査官は、この出願の発明は８群に区分されると認定したが、追加手数料異議の申立ての決定の結果、以下の７群となった。

1．請求の範囲 1-5, 8-10
2．請求の範囲 6, 7, 11, 12
3．請求の範囲13, 14
4．請求の範囲15, 16
5．請求の範囲17
6．請求の範囲18
7．請求の範囲19

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☒ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

請求の範囲 1-5, 8-10

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☒ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2000-122539 A　(松下電器産業株式会社) 28. 4月. 2000(28.04.00), 第18,44,45段落（ファミリなし）	1-5,8-10
A	一松信 監修, データ保護と暗号化の研究 コンピュータ・ネットワークの安全性, 日本経済新聞社, 29.7月.1983(29.07.83), p.201-206　(特にp.204 3データ暗号鍵の登録 を参照)	1-5,8-10

特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002年1月3日 (03.01.2002)

PCT

(10) 国際公開番号
WO 02/01790 A1

(51) 国際特許分類[7]: H04L 9/00, G11B 20/10, G06F 15/00

(21) 国際出願番号: PCT/JP01/05484

(22) 国際出願日: 2001年6月27日 (27.06.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:

特願2000-196080	2000年6月29日 (29.06.2000)	JP
特願2000-203375	2000年7月5日 (05.07.2000)	JP
特願2000-203376	2000年7月5日 (05.07.2000)	JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006 Osaka (JP).

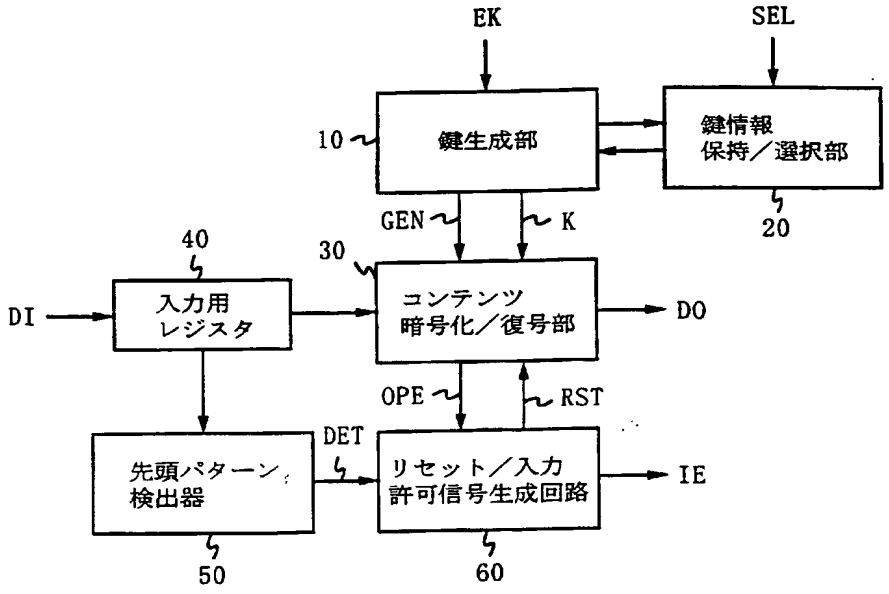
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 岡山睦之 (OKAYAMA, Mutsuyuki) [JP/JP]; 〒612-8012 京都府京都市伏見区桃山町遠山24番12号 Kyoto (JP). 柳澤玲互 (YANAGISAWA, Ryogo) [JP/JP]; 〒547-0024 大阪府大阪市平野区瓜破三丁目2-85 エレガントコーポラス403号 Osaka (JP). 石原秀志 (ISHIHARA, Hideshi) [JP/JP]; 〒576-0054 大阪府交野市幾野一丁目10番120号 Osaka (JP).

[続葉有]

(54) Title: COPYRIGHT PROTECTIVE DEVICE AND METHOD

(54) 発明の名称: 著作権保護装置及び方法



10...KEY CREATING SECTION
20...KEY INFORMATION HOLDING/SELECTING SECTION
40...INPUT REGISTER
30...CONTENT ENCRYPTING/DECRYPTING SECTION
50...FIRST PATTERN DETECTOR
60...RESET/INPUT PERMISSION SIGNAL GENERATING CIRCUIT

(57) Abstract: A key creating section (10) creates a key K used for encryption according to a set of data EK on encrypted keys. A key information holding/selecting section (20) holds the created key and an intermediate key obtained when the key is created and outputs key information held according to selection information SEL. The key information is held in, e.g., a storage circuit in, an integrated circuit in the form in which the key information is not recognized as a key. A content encrypting/decrypting section (30) suppresses the output of the result of encryption DO during the key creation. A reset/input permission signal generating circuit (60) brings an input permission signal IE into a prohibited state if the first pattern is detected during the encryption of an input signal DI, and outputs a reset signal RST after the encryption.

[続葉有]

WO 02/01790 A1

(74) 代理人: 小笠原史朗(OGASAWARA, Shiro); 〒564-0053 大阪府吹田市江の木町3番11号 第3ロンヂェビル Osaka (JP).

(81) 指定国 (国内): CN, KR, US.

添付公開書類:
— 国際調査報告書
— 補正書

(57) 要約:

鍵生成部１０は、暗号化された鍵データ群ＥＫに基づき、暗号処理に使用する鍵Ｋを生成する。鍵情報保持／選択部２０は、生成された鍵と、鍵を生成する際に得られた中間鍵とを保持し、選択情報ＳＥＬに応じて保持した鍵情報を出力する。鍵情報は、鍵として認識できない形式で、例えば集積回路内部の記憶回路に保持される。コンテンツ暗号化／復号部３０は、鍵生成中は暗号処理結果ＤＯの出力を抑制する。リセット／入力許可信号生成回路６０は、入力信号ＤＩの暗号処理中に先頭パターンが検出されたときには、入力許可信号ＩＥを禁止状態に切り替え、暗号処理が完了した後にリセット信号ＲＳＴを出力する。

明細書

著作権保護装置及び方法

技術分野

本発明は、著作権保護装置および著作権保護方法に関し、より特定的には、音声や画像等のデータを含んだコンテンツに対して記録、再生、送信、受信等の処理を行う際に、コンテンツの著作権を保護する著作権保護装置および著作権保護方法に関する。

背景技術

従来、コンテンツに含まれる音声や画像等のデータは、アナログデータであった。アナログデータに対して記録、再生、送信、受信等の処理を行うと、データの品質が劣化する。このため、コンテンツの著作権保護は、従来は大きな問題とはされていなかった。しかし、近年ディジタル技術が一層進歩し、コンテンツに含まれる文字や音声や画像等のデータをディジタル化することが、広く一般的に行われるようになっている。ディジタルデータに対して記録、再生、送信、受信等の処理を行っても、データの品質はほとんど劣化しない。このため、コンテンツの著作権保護は、近年大きな問題とされるようになっている。

この問題を解決するために、様々な著作権保護技術が開発され、実用化されている。例えば、ＤＥＳ（Data Encryption Standard）暗号やＲＳＡ（Rivest Shamir Adleman

）暗号等が実用化されている。これらの暗号化技術の詳細は、例えば、「現代暗号理論入門」電子情報通信学会編、池野信一　他、１９９８年１１月．に記載されているので、ここでは説明を省略する。著作権保護装置の具体例は、例えば、日本国特開平８－２８７０１４号公報に記載されている。

暗号化技術では、コンテンツを暗号化し、暗号化されたコンテンツを復号するための暗号鍵（以下、「鍵」という）の管理は、極めて重要である。そこで近年、記録メディアに記録されたコンテンツ用の鍵を管理する技術として、ＣＰＲＭ（Content Protection for Recordable Media）やＣＰＰＭ（Content Protection for Prerecorded Media）等の規格が提案されている。ＣＰＲＭやＣＰＰＭでは、複数の中間鍵を求め、求めた中間鍵に演算処理を行うことにより、コンテンツの暗号化または暗号復号する際に使用される鍵（以下、「最終鍵」という）が生成される。ＣＰＲＭでは、媒体鍵（Media Key）と媒体独自鍵（Media Unique Key）とが中間鍵として使用され、表題鍵（Title Key）が最終鍵となる。ＣＰＰＭでは、媒体鍵が中間鍵として使用され、アルバム独自鍵（Album Unique Key）が最終鍵となる。

ＣＰＲＭとＣＰＰＭの詳細は、次の４冊の仕様書に記載されている。第１の仕様書は、″Content Protection for Recordable Media Specification - Introduction and Common Cryptographic Elements″, Revision 0.92, April 18, 2000.である。第２の仕様書は、″Content Protection

for Recordable Media Specification - DVD Book", Revision 0.92, April 18, 2000.である。第３の仕様書は、"Content Protection for Prerecorded Media Specification - Introduction and Common Cryptographic Elements", Revision 0.91, April 18, 2000. である。第４の仕様書は、"Content Protection for Prerecorded Media Specification - DVD Book", Revision 0.91, April 18, 2000. である。これらの仕様書は、いずれも一般に公開されている。

ＣＰＲＭやＣＰＰＭ等の鍵管理技術では、鍵の生成に複雑な演算処理を行うため、以下に示す３つの問題が生じる。第１の問題点は、鍵生成処理が複雑であるため、最終鍵を生成するまでに多大な時間を要することである。例えば、ＣＰＲＭやＣＰＰＭでは、最終鍵を生成するために、複数の中間鍵を生成し、認証や検証等の処理を行う必要がある。鍵の生成に時間がかかることは、複数のメディアを同時に再生装置に装着し、複数のメディアに跨るランダム再生を行う場合に、非常に大きな問題となる。この問題点を解決するため、日本国特開平８－２８７０１４号公報には、中間鍵を保持して処理する方法が開示されている。しかし、この方法では、中間鍵がローカルバス上に読み取り可能な状態で現れるため、暗号強度の点で大きな課題があった。

第２の問題点は、鍵の生成に時間がかかることに起因にして、鍵の生成と同時にコンテンツの暗号化または暗号復号を行うと、鍵の生成が間に合わないために誤った暗号処

理結果が得られることである。すなわち、鍵の生成中にコンテンツデータをコンテンツ暗号化部に入力しても、コンテンツ暗号化部は、本来の暗号化結果とは全く異なる結果を生成して出力する。また、鍵の生成中に暗号化されたコンテンツデータをコンテンツ復号部に入力しても、コンテンツ復号部は、正しいコンテンツデータを生成できず、誤った結果を生成して出力する。

また、出力制御の問題について言えば、コンテンツの暗号化または暗号復号を行うか否かを示す識別情報がコンテンツデータ自体に含まれている場合に、著作権保護装置の出力信号を制御する方法は知られていない。例えば、日本国特開平１１－１２６４２３号公報には、コンテンツデータに含まれるコピービットを識別情報として使用し、これを用いてコピー可能か否かを判断する方法が開示されている。この方法では、コピー可能か否かを判断できた時点で、コンテンツデータは、コンテンツ暗号化部またはコンテンツ復号部に入力される。しかし、コンテンツ暗号化部またはコンテンツ復号部が、識別情報を検出する機能を内部に有している場合には、外部からコンテンツ暗号化部またはコンテンツ復号部に識別信号を入力することができないため、コンテンツの暗号化データまたは復号データを出力することができないという問題があった。

第３の問題点は、著作権保護装置の信号処理回路に関するものである。ディジタル信号処理回路は、一般にエラー発生等の異常事態を考慮して設計される。例えば、信号処理回路は、異常事態の発生を考慮して適宜定期的にリセッ

トを行い、たとえ異常状態に陥っても正しいデータが入力されたときには元通り正しく動作するように設計される。日本国特開平７－１４３４８９号公報には、このような手法の一例として、データに含まれる所定のコードパターンを検出したときに回路をリセットする方法が開示されている。しかし、コードパターンを検出した時点で直ちに回路をリセットすると、回路内部のレジスタ等の記憶回路に記憶されている正しいデータまでも消去されてしまい、正しく信号処理を行うことができないという問題があった。

また、信号処理回路の問題について言えば、入力許可信号を用いて入力信号を制御する従来の信号処理回路は、入力許可信号が非アクティブになれば、内部回路でもデータをホールドするように構成されていた。しかし、何らかの理由で、入力許可信号が非アクティブになった後もデータが入力される場合、従来の信号処理回路では、入力許可信号が非アクティブになった後に入力されたデータを欠落させてしまうという問題があった。

それ故に、本発明の第一の目的は、暗号強度を維持しながら中間鍵または最終鍵を高速に生成する著作権保護装置を提供することである。このような著作権保護装置は、複数のメディアを同時に再生装置に装着し、メディアを跨るランダム再生を行う際に、特に有効となる。本発明の第二の目的は、鍵の生成と同時に、コンテンツの先頭部分を欠落させることなく、正しい鍵でコンテンツを暗号化または暗号復号する著作権保護装置を提供することである。本発明の第三の目的は、定期的にリセットを行うためのコード

パターンが入力データに挿入されている場合に、リセットを正しく行い、たとえ異常状態に陥っても正しいデータが入力されたときには正しく動作する著作権保護装置を提供することである。また、第三の目的とも関連して、本発明は、入力許可信号が非アクティブになった後にデータが入力される場合でも、そのデータを欠落させることなく、首尾良く処理する著作権保護装置を提供することを目的とする。

発明の開示

本発明は、上記のような目的を達成するために、以下に述べるような特徴を有している。

本発明の第１の局面は、コンテンツの暗号化または暗号復号を行う著作権保護装置であって、コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、

鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、鍵を生成するための中間鍵および鍵の少なくとも一方を、鍵として認識できない形式で保持する保持手段とを備える。

このような第１の局面によれば、中間鍵と鍵とは、鍵として使用者から認識できない形式で保持手段に保持される。したがって、生成した中間鍵や鍵を利用することにより、２回目以降の鍵生成を短時間に行うことができる。また、中間鍵と鍵とは、使用者から認識できない形式で保持されるので、鍵の暗号強度が損なわれることがない。

この場合、鍵生成手段は、複数のメディアのそれぞれに

ついて鍵を生成し、暗号処理手段は、各メディアごとに生成された鍵を用いて、コンテンツに暗号処理を行うこととしてもよい。これにより、複数のメディアを装着する装置において、複数のメディアに跨るランダムアクセスを短時間で行うことができる。

また、保持手段は、中間鍵および鍵を集積回路内の記憶回路に保持することとしてもよい。これにより、中間鍵と鍵とを外部から認識できない状態で保持することができる。

本発明の第２の局面は、コンテンツの暗号化または暗号復号を行う著作権保護装置であって、コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、鍵を生成するための中間鍵および鍵の少なくとも一方を、暗号化して保持する保持手段とを備える。

このような第２の局面によれば、中間鍵と鍵とは、暗号化された状態で保持手段に保持される。したがって、生成した中間鍵や鍵を利用することにより、２回目以降の鍵生成を短時間に行うことができる。また、中間鍵と鍵とは、暗号化された状態で保持されるので、鍵の暗号強度を高めることができる。さらに、集積回路外部の記憶回路に暗号化した鍵を保持させることができるので、保持する鍵の量が、集積回路内部の記憶回路の量に制限されることがない。

この場合、鍵生成手段は、複数のメディアのそれぞれについて鍵を生成し、暗号処理手段は、各メディアごとに生

成された鍵を用いて、コンテンツに暗号処理を行うこととしてもよい。これにより、複数のメディアを装着する装置において、複数のメディアに跨るランダムアクセスを短時間で行うことができ、かつ、鍵の暗号強度を高めることができる。

本発明の第３の局面は、コンテンツの暗号化または暗号復号を行う著作権保護装置であって、行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより、コンテンツに暗号処理を行うための鍵と、鍵を生成するための中間鍵とを生成する鍵生成手段と、鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、中間鍵および鍵生成用データの少なくとも一方を保持する保持手段とを備える。

このような第３の局面によれば、中間鍵と鍵とは、行列状に形成された鍵生成用データから複雑なアルゴリズムで算出され、鍵として使用者から認識できない形式で保持手段に保持される。したがって、生成した中間鍵や鍵を利用することにより、複雑な鍵生成アルゴリズムを採用した場合でも、２回目以降の鍵生成を短時間に行うことができる。また、中間鍵と鍵とは、使用者から認識できない形式で保持されるので、鍵の暗号強度が損なわれることがない。

この場合、鍵生成手段は、複数のメディアのそれぞれについて鍵を生成し、暗号処理手段は、各メディアごとに生成された鍵を用いて、コンテンツに暗号処理を行い、保持手段は、中間鍵および鍵生成用データを各メディアごとに保持することとしてもよい。これにより、複数のメディア

を装着する装置において、複雑な鍵生成アルゴリズムを採用した場合でも、複数のメディアに跨るランダムアクセスを短時間で行うことができる。

本発明の第４の局面は、コンテンツの暗号化または暗号復号を行う著作権保護方法であって、コンテンツに暗号処理を行うための鍵を生成する鍵生成ステップと、鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、鍵を生成するための中間鍵および鍵の少なくとも一方を、鍵として認識できない形式で保持する保持ステップとを備える。

このような第４の局面によれば、中間鍵と鍵とは、鍵として使用者から認識できない形式で保持ステップで保持される。したがって、生成した中間鍵や鍵を利用することにより、２回目以降の鍵生成を短時間に行うことができる。また、中間鍵と鍵とは、使用者から認識できない形式で保持されるので、鍵の暗号強度が損なわれることがない。

この場合、鍵生成ステップは、複数のメディアのそれぞれについて鍵を生成し、暗号処理ステップは、各メディアごとに生成された鍵を用いて、コンテンツに暗号処理を行うこととしてもよい。これにより、複数のメディアを装着する装置において、複数のメディアに跨るランダムアクセスを短時間で行うことができる。

本発明の第５の局面は、コンテンツの暗号化または暗号復号を行う著作権保護方法であって、コンテンツに暗号処理を行うための鍵を生成する鍵生成ステップと、鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、鍵

を生成するための中間鍵および鍵の少なくとも一方を、暗号化して保持する保持ステップとを備える。

このような第５の局面によれば、中間鍵と鍵とは、暗号化された状態で保持ステップで保持される。したがって、生成した中間鍵や鍵を利用することにより、２回目以降の鍵生成を短時間に行うことができる。また、中間鍵と鍵とは、暗号化された状態で保持されるので、鍵の暗号強度を高めることができる。さらに、集積回路外部の記憶回路に暗号化した鍵を保持させることができるので、保持する鍵の量が、集積回路内部の記憶回路の量に制限されることがない。

本発明の第６の局面は、コンテンツの暗号化または暗号復号を行う著作権保護方法であって、行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより、コンテンツに暗号処理を行うための鍵と、鍵を生成するための中間鍵とを生成する鍵生成テップと、鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、中間鍵および鍵生成用データの少なくとも一方を保持する保持ステップとを備える。

このような第６の局面によれば、中間鍵と鍵とは、行列状に形成された鍵生成用データから複雑なアルゴリズムで算出され、鍵として使用者から認識できない形式で保持ステップで保持される。したがって、生成した中間鍵や鍵を利用することにより、複雑な鍵生成アルゴリズムを採用した場合でも、２回目以降の鍵生成を短時間に行うことができる。また、中間鍵と鍵とは、使用者から認識できない形

式で保持されるので、鍵の暗号強度が損なわれることがない。

この場合、鍵生成ステップは、複数のメディアのそれぞれについて鍵を生成し、暗号処理ステップは、各メディアごとに生成された鍵を用いて、コンテンツに暗号処理を行い、保持ステップは、中間鍵および鍵生成用データを各メディアごとに保持することとしてもよい。これにより、複数のメディアを装着する装置において、複雑な鍵生成アルゴリズムを採用した場合でも、複数のメディアに跨るランダムアクセスを短時間で行うことができる。

本発明の第７の局面は、コンテンツの暗号化または暗号復号を行う著作権保護装置であって、コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段と、暗号処理を行うか否かを示す識別情報を含んだコンテンツが入力され、識別情報に従って鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段とを備え、暗号処理手段は、通知信号が鍵生成中を示す場合は、暗号処理結果の出力を抑制することを特徴とする。

本発明の第８の局面は、コンテンツの暗号化または暗号復号を行う著作権保護装置であって、コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段と、暗号処理を行うか否かを示す識別信号を含んだコンテンツが入力され、識別信号に従って鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段と、通知信号が鍵生成

中を示す場合は、暗号処理手段に入力されたコンテンツを選択し、それ以外の場合は、暗号処理手段から出力された暗号処理結果を選択して出力する選択手段とを備える。

このような第７および第８の局面によれば、鍵生成中は、暗号処理手段で求めた結果は、次段の処理手段に出力されない。したがって、誤った鍵で暗号処理を行った結果を出力しないので、次段の処理手段に悪影響を及ぼすことがない。第８の局面は、高能率符号化された後に部分的に暗号化されたコンテンツを記録したディスクを再生する場合に、特に有効である。この場合、コンテンツの高能率符号化を復号するためのヘッダ情報が少しでも出力されるため、最終的にコンテンツを早く出力することができる。

本発明の第９の局面は、コンテンツの暗号化または暗号復号を行う著作権保護装置であって、コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段と、暗号処理を行うか否かを示す識別信号を含んだコンテンツが入力され、識別信号に従って鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段とを備え、暗号処理手段は、通知信号が鍵生成中を示す場合は、コンテンツの入力を制御する入力許可信号を入力禁止状態に切り替えることを特徴とする。

本発明の第１０の局面は、コンテンツの暗号化または暗号復号を行う著作権保護装置であって、コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、暗号処理を行うか否かを示す識別信号を含んだコンテンツが入力され

、識別信号に従って鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段とを備え、鍵生成手段は、鍵生成中は、コンテンツの入力を制御する入力許可信号を入力禁止状態に切り替えることを特徴とする。

このような第９および第１０の局面によれば、鍵生成中は、コンテンツの入力が禁止されるので、暗号処理手段で求めた結果は、次段の処理手段に出力されない。したがって、誤った鍵で暗号処理を行った結果を出力しないので、次段の処理手段に悪影響を及ぼすことがない。第９および第１０の局面は、コンテンツを暗号化してディスクに記録する場合に、特に有効である。この場合、暗号処理手段は、鍵生成中に生成した誤ったデータを出力することなく、かつ、コンテンツの先頭部分を正しく暗号化した結果を途切れることなく出力することができる。

本発明の第１１の局面は、複数のシンボルごとに処理単位の先頭を示す先頭パターンを含んだ入力信号を処理する信号処理装置であって、順次入力された入力信号を保持するレジスタと、レジスタに保持された入力信号に、先頭パターンが含まれていることを検出する先頭パターン検出手段と、レジスタを経由して供給された入力信号に所定の信号処理を行うとともに、入力信号を処理中か否かを通知する信号処理手段と、先頭パターン検出手段が先頭パターンを検出したときに信号処理手段が処理中でない場合には、リセット信号を信号処理手段に出力し、先頭パターン検出手段が先頭パターンを検出したときに信号処理手段が処理中である場合には、入力を制御する入力許可信号を入力禁

止状態に切り替えるとともにリセット待機状態に遷移し、リセット待機状態で信号処理手段における処理が完了したときに、リセット信号を信号処理手段に出力する制御信号生成手段とを備える。

このような第１１の局面によれば、定期的にリセットを行うためのコードパターンが入力データに挿入されている場合に、リセットを正しく行い、たとえ異常状態に陥っても正しいデータが入力たときには正しく動作することができる。

本発明の第１２の局面は、入力許可信号に従ってシンボルごとに入力される入力信号を処理する信号処理装置であって、入力許可信号が入力禁止状態に変化した後に高々ｃシンボル分の入力信号が入力され、入力信号を一度にｂシンボル分処理するとともに、内部処理のオーバーフロー状態を通知する信号処理手段と、信号処理手段における処理がオーバーフロー状態となったときに、入力許可信号を入力禁止状態に切り替える入力許可信号生成手段と、ａシンボル分の入力信号を保持し、入力許可信号が入力許可状態であるときにはｂシンボルを信号処理手段に出力し、値ａと値ｂと値ｃとにはａ≧（ｂ＋ｃ）なる関係が成立し、入力許可信号と当該信号を１クロックサイクル遅延させた信号との論理和信号をロード信号として用いるレジスタとを備える。

本発明の第１３の局面は、入力許可信号に従ってシンボルごとに入力される入力信号を処理する信号処理装置であって、入力許可信号が入力禁止状態に変化した後に高々ｃ

シンボル分の入力信号が入力され、入力信号に所定の処理を行うとともに、入力信号を受け入れ可能か否かを通知する信号処理手段と、入力信号を記憶し、記憶した入力信号を信号処理手段に対して出力するメモリと、信号処理手段が入力信号を受け入れ可能である場合には、データが読み出されるようにメモリを制御し、未だ読み出されていないデータには上書きしないように書き込み制御を行いながら、書き込みアドレスと読み出しアドレスとを出力するメモリ制御手段と、メモリ制御手段から出力された書き込みアドレスと読み出しアドレスとに基づき算出した書き込み余裕量が少なくともｃシンボルになったときに、入力許可信号を入力禁止状態に切り替える入力許可信号生成手段とを備える。

このような第１２および第１３の局面によれば、入力許可信号が非アクティブになった後にデータが入力される場合でも、そのデータを欠落させることなく、首尾良く処理することができる。

図面の簡単な説明

図１は、本発明の第１の実施形態に係る著作権保護装置の構成を示すブロック図である。

図２は、本発明の実施形態に係る著作権保護装置の鍵生成部のブロック図である。

図３は、本発明の実施形態に係る著作権保護装置の鍵情報保持／選択部のブロック図である。

図４は、本発明の第１の実施形態に係る著作権保護装置

の出力制御機能を説明するためのブロック図である。

図５は、本発明の第１の実施形態に係る著作権保護装置のリセット／入力制御機能を説明するためのブロック図である。

図６は、本発明の実施形態に係る著作権保護装置の他の鍵情報保持／選択部のブロック図である。

図７は、再生処理時間を比較する図である。

図８は、本発明の第４から第６の実施形態に係る著作権保護装置の媒体鍵ブロックに含まれる計算媒体鍵レコードのデータ構造図である。

図９は、本発明の第４から第６の実施形態に係る著作権保護装置の媒体鍵ブロックに含まれる条件付き計算媒体鍵レコードのデータ構造図である。

図１０は、本発明の第４および第５の実施形態に係る著作権保護装置の鍵情報生成および鍵情報保持の動作を示すフローチャートである。

図１１は、本発明の第６の実施形態に係る著作権保護装置の鍵情報生成および鍵情報保持の動作を示すフローチャートである。

図１２は、本発明の第６の実施形態に係る著作権保護装置の鍵情報生成および鍵情報保持の他の動作を示すフローチャートである。

図１３は、本発明の第７の実施形態に係る著作権保護装置の出力制御機能を説明するためのブロック図である。

図１４は、本発明の第７の実施形態に係る著作権保護装置の出力信号のタイミングチャートである。

図１５は、本発明の第８の実施形態に係る著作権保護装置の出力制御機能を説明するためのブロック図である。

図１６は、本発明の第８の実施形態に係る著作権保護装置の入力信号のタイミングチャートである。

図１７は、本発明の第８の実施形態の変形例に係る著作権保護装置の出力制御機能を説明するためのブロック図である。

図１８は、本発明の第９の実施形態に係る著作権保護装置の入力制御機能を説明するためのブロック図である。

図１９は、本発明の第９の実施形態に係る著作権保護装置の入力信号のタイミングチャートである。

図２０は、本発明の第１０の実施形態に係る著作権保護装置のリセット／入力制御機能を説明するためのブロック図である。

図２１は、本発明の第１１の実施形態に係る著作権保護装置の入力制御機能を説明するためのブロック図である。

図２２は、本発明の第１１の実施形態の変形例に係る著作権保護装置のリセット／入力制御機能を説明するためのブロック図である。

発明を実施するための最良の形態

（第１の実施形態）

図１は、本発明の第１の実施形態に係る著作権保護装置の構成を示すブロック図である。図１に示す著作権保護装置は、鍵生成部１０、鍵情報保持／選択部２０、コンテンツ暗号化／復号部３０、入力用レジスタ４０、先頭パター

ン検出部５０、および、リセット／入力許可信号生成回路６０を備える。この著作権保護装置は、鍵情報Ｋを生成し、生成した鍵情報Ｋを用いて入力データＤＩに暗号化処理または暗号復号処理を行い、出力データＤＯを出力する。以下では、上述した３つの課題（鍵生成、出力制御、および、リセット／入力制御）と対応づけて、図１に示す著作権保護装置の特徴を説明する。

まず、第１の特徴である鍵生成時間の短縮について説明する。図２は、鍵生成部１０の構成を示すブロック図である。図２において、鍵生成部１０は、中間鍵処理部１１と最終鍵処理部１２とを備える。図３は、鍵情報保持／選択部２０の構成を示すブロック図である。図３において、鍵情報保持／選択部２０は、選択回路２１とレジスタ回路２２とを備える。

本実施形態を容易に理解するために、例として、ＤＶＤ記録再生装置における鍵の生成について説明する。以下に示す鍵生成アルゴリズムでは、装置鍵Ａ、媒体鍵Ａ、媒体独自鍵Ａ、表題鍵Ａ、内容鍵Ａが使用される。各機器は、それぞれ固有の装置鍵を有している。媒体鍵Ａは、各装置において装置鍵Ａで暗号化され、ＤＶＤメディアに記録される。装置鍵は機器ごとに設定されるため、１枚のＤＶＤメディアには、各機器の装置鍵で暗号化された複数の媒体鍵が記録される。複数の媒体鍵は、鍵データ群として扱われる。

ＤＶＤメディアに暗号化された状態で記録されている媒体鍵Ａは、ＤＶＤメディアから再生され、暗号化された鍵

データ群ＥＫとして鍵生成部１０に入力される。このとき、装置鍵Ａは、既に何らかの手段で鍵生成部１０に入力されているとする。装置鍵Ａは、例えば、予め固定的に入力されていてもよく、あるいは、ある種の変換された形式で外部から供給され、鍵生成部１０で復元されることとしてもよい。鍵生成部１０は、暗号化された媒体鍵Ａを装置鍵Ａで暗号復号し、媒体鍵Ａを求める。また、鍵生成部１０には、暗号化された鍵データ群ＥＫとして、所定の値ａが外部から入力される。鍵生成部１０は、入力された値ａを用いて、媒体鍵Ａを媒体独自鍵Ａに変換する。さらに、鍵生成部１０には、暗号化された表題鍵Ａが入力される。鍵生成部１０は、暗号化された表題鍵Ａを媒体独自鍵Ａで暗号復号し、表題鍵Ａを求める。

図２と対応づけて、鍵生成手順を再度説明する。図２において、鍵生成部１０には、鍵情報ＫＩとして装置鍵Ａが入力され、暗号化された中間鍵ＥＫ１として、暗号化された媒体鍵Ａが入力される。中間鍵処理部１１は、暗号化された中間鍵ＥＫ１を鍵情報ＫＩで暗号復号し、中間鍵ＫＭである媒体鍵Ａを求める。また、鍵生成部１０には、暗号化された中間鍵ＥＫ１として、値ａが入力される。なお、値ａは、実際に暗号化されている必要性はない。中間鍵処理部１１は、値ａを用いて媒体鍵Ａに対して変換を行い、新たな中間鍵ＫＭである媒体独自鍵Ａを求める。さらに鍵生成部１０には、暗号化された最終鍵ＥＫ２として、暗号化された表題鍵Ａが入力される。最終鍵処理部１２は、暗号化された表題鍵Ａを媒体独自鍵Ａで暗号復号し、最終鍵

Ｋである表題鍵Ａを求める。

求めた表題鍵Ａは、最終鍵Ｋとしてコンテンツ暗号化／復号部３０に入力される。コンテンツ暗号化／復号部３０は、表題鍵Ａを用いて、暗号化処理または暗号復号処理を行う。

一方、求めた媒体鍵Ａと媒体独自鍵Ａと表題鍵Ａとは、鍵情報保持／選択部２０に供給され、選択回路２１を経てレジスタ回路２２に記憶される。鍵情報保持／選択部２０では、外部から供給された選択情報ＳＥＬに応じて、選択回路２１が動作する。選択回路２１は、レジスタ回路２２に記憶された数種類の鍵を選択し、鍵生成部１０に出力する。例えば、暗号文データの復号を中断した後に、再び暗号文データを復号する場合には、レジスタ回路２２に記憶された鍵を呼び出せばよい。このように、２回目以降に鍵を生成する場合には、記憶回路から鍵を呼び出すだけでよいので、短時間で鍵情報を生成することができる。

次に、第２の特徴である鍵生成中の出力制御について説明する。図４は、図１に示すブロック図から鍵生成部１０とコンテンツ暗号化／復号部３０とを取り出して示した図である。コンテンツ暗号化／復号部３０が、入力データＤＩを暗号復号する場合について説明する。

上述したように、鍵生成部１０は、最終鍵Ｋとして表題鍵Ａをコンテンツ暗号化／復号部３０に出力する。コンテンツ暗号化／復号部３０には、コンテンツを暗号化して求めた暗号文データＤＩが入力される。コンテンツ暗号化／復号部３０は、入力された暗号文データＤＩから一部の情

報を抽出し、これを用いて表題鍵Ａを内容鍵Ａに変換する。さらに、コンテンツ暗号化／復号部３０は、暗号文データＤＩに含まれる識別情報に基づき、暗号復号を行うか否かを判断する。コンテンツ暗号化／復号部３０は、復号すべきと判断した場合には、暗号文データＤＩを内容鍵Ａで暗号復号し、平文データＤＯを出力する。

鍵生成部１０は、装置鍵Ａや媒体鍵Ａ等の中間鍵の生成を開始してから、媒体独自鍵Ａ等の中間鍵または表題鍵Ａ等の最終鍵を生成し終えるまでの間、鍵生成期間通知信号ＧＥＮをアクティブにしてコンテンツ暗号化／復号部３０に出力する。コンテンツ暗号化／復号部３０は、信号ＧＥＮがアクティブである場合、すなわち、鍵生成中である場合には、暗号復号処理を行った結果の平文データＤＯを出力しない。

このように、誤った鍵で暗号化または暗号復号した結果を出力しないため、次段の処理手段に悪影響を及ぼすことがない。

次に、第３の特徴であるリセット／入力制御について説明する。図５は、図１に示すブロック図から、コンテンツ暗号化／復号部３０、入力用レジスタ４０、先頭パターン検出器５０、および、リセット／入力許可信号生成回路６０を取り出して示した図である。入力用レジスタ４０は、第１から第４のレジスタ４１～４４を含んでいる。

本実施形態を容易に理解するために、図５に示す著作権保護装置には、データは、８ビット並列に２０４８バイトを一単位として入力されると仮定する。また、一単位のデ

ータの先頭には、３２ビットの先頭パターンＰが配置されると仮定する。先頭パターンＰの値は任意でよいが、例えば、ＤＶＤレコーディング規格やＤＶＤビデオやＤＶＤオーディオプレーヤ等のＤＶＤ機器のフォーマットに準拠して、000001BA（１６進数）と仮定する。

図５に示す著作権保護装置には、２０４８バイトで一単位となる入力データＤＩが、１バイトづつ順次入力される。入力されたデータは、第１から第４のレジスタ４１～４４に順次保持される。４バイトのデータが入力されると、入力データは、第１から第４のレジスタ４１～４４から、４バイト同時にコンテンツ暗号化／復号部３０に入力される。コンテンツ暗号化／復号部３０は、入力されたデータに所定の処理を行い、その結果として出力データＤＯを出力する。このとき同時に、コンテンツ暗号化／復号部３０は、回路自身が動作中か否かを、すなわち、入力信号を処理中か否かを示す通知信号ＯＰＥを出力する。通知信号ＯＰＥは、リセット／入力許可信号生成回路６０に入力される。

先頭パターン検出器５０は、第１から第４のレジスタ４１～４４に蓄積されたデータを監視し、先頭パターンＰを検出した旨を示す検出信号ＤＥＴを出力する。検出信号ＤＥＴは、リセット／入力許可信号生成回路６０に入力される。

リセット／入力許可信号生成回路６０は、通知信号ＯＰＥが処理中でない旨を示している状態で検出信号ＤＥＴを受けたときには、コンテンツ暗号化／復号部３０にリセッ

ト信号ＲＳＴを出力する。

これに対して、リセット／入力許可信号生成回路６０は、通知信号ＯＰＥが処理中を示している状態で検出信号ＤＥＴを受けたときには、入力許可信号ＩＥを非アクティブにして入力信号を停止させ、リセット待機状態に遷移する。より詳細には、リセット／入力許可信号生成回路６０は、リセットを行う準備した旨を示す信号を内部で保持する。このリセットを行う準備をした旨を示す信号を内部で保持することを「リセット待機」と呼ぶ。

リセット／入力許可信号生成回路６０は、リセット待機状態で通知信号ＯＰＥが処理完了に変化したときに、リセット信号ＲＳＴをコンテンツ暗号化／復号部３０に出力するとともに、リセット待機状態を解除する。また、リセット／入力許可信号生成回路６０は、コンテンツ暗号化／復号部３０における処理がオーバーフロー状態となったときには、入力許可信号ＩＥを非アクティブにして、入力信号を停止させる。

このように、定期的に正しくリセットを行い、異常状態に陥っても正しいデータが入力されたときには、正しく動作することができる。

なお、本実施形態では、暗号化されたコンテンツを暗号復号する場合について説明したが、逆に平文データのコンテンツを暗号化する場合でも同様の構成を採用することができる。また、鍵生成アルゴリズムは、媒体独自鍵Ａと内容鍵Ａを両方とも使用しないものでもよく、片方のみ使用するものでもよい。さらに、表題鍵Ａを生成する過程は、

より複雑なものであってもよい。

また、本実施形態では、入力データの一単位は、２０４８バイトであるとしたが、例えば１０２４バイトや１８８バイトや１９４バイト等、任意の長さでよい。また、先頭パターンＰを３２ビットの000001BA（１６進数）としたが、例えば、３２ビットの000001BB、00000100（１６進数）、２８ビットの000001e（１６進数）、８ビットの４７（１６進数）等、任意の値でもよい。また、コンテンツ暗号化／復号部３０は、複数の部分回路で構成されていてもよい。

以下、本発明の他の実施形態を説明するが、第２から第６の実施形態は上記第１の特徴に関するものであり、第７および第８の実施形態は上記第２の特徴に関するものであり、第９から第１１の実施形態は上記第３の特徴に関するものである。なお、各実施形態の構成要素のうち、先に示した実施形態と同一の構成要素については、同一の参照符号を付して説明を省略する。

（第２の実施形態）

本発明の第２の実施形態は、鍵情報保持／選択部２０の構成に特徴がある。図６は、本実施形態に係る鍵情報保持／選択部２０のブロック図である。図６に示す鍵情報保持／選択部２０は、暗号化／復号回路２３を備える。

本実施形態でも、第１の実施形態と同様に、装置鍵Ａ、媒体鍵Ａ、媒体独自鍵Ａ、表題鍵Ａおよび内容鍵Ａを用いたアルゴリズムが使用される。鍵生成部１０は、媒体鍵Ａ、媒体独自鍵Ａ等の中間鍵と、表題鍵Ａ等の最終鍵とを、

鍵情報保持／選択部２０に出力する。鍵情報保持／選択部２０は、これらの鍵を暗号化／復号回路２３で暗号化し、その結果を出力する。鍵情報保持／選択部２０の出力先は、例えば、集積回路内部の記憶回路でも、集積回路外部の記憶回路でもよい。集積回路内部の記憶回路の場合には、暗号化／復号回路２３の次段に、図３で示したような回路群が装着される。

鍵情報が必要となったときには、集積回路内部または集積回路外部の記憶回路に暗号化された状態で記憶されている鍵情報のうち、必要な鍵情報が読み出され、暗号化／復号回路２３で暗号復号されて、鍵生成部１０に入力される。

例えば、媒体独自鍵Ａを保持する場合について説明する。媒体独自鍵Ａが鍵生成部１０における鍵生成手順に従って生成され、鍵情報保持／選択部２０に入力されたとする。鍵情報保持／選択部２０に入力された媒体独自鍵Ａは、暗号化／復号回路２３によって暗号化され、例えば、集積回路外部の記憶回路に保持される。その後、媒体独自鍵Ａが必要となった場合には、暗号化された媒体独自鍵Ａが、集積回路外部の記憶回路から読み出され、暗号化／復号回路２３において暗号復号される。このようにして得られた媒体独自鍵Ａは、鍵生成部１０に供給される。

このように本実施形態に係る著作権保護装置によれば、２回目以降に鍵を生成する場合には、鍵を鍵生成部１０における手順に従って生成するよりも短時間で生成できる。また、鍵は暗号化された状態で保持されるので、第１の実

施形態と比べて、鍵の暗号強度を高めることができる。さらに、集積回路外部の記憶回路に暗号化した鍵を保持させることができるので、保持する鍵の量が、集積回路内部の記憶回路の量に制限されることがない。

（第３の実施形態）

本発明の第３の実施形態は、複数のメディアを装着するために、各メディアごとに生成された鍵情報を保持することを特徴とする。具体的には、鍵情報保持／選択部２０が、複数のメディアのそれぞれについて生成された鍵情報を保持する。

本実施形態を容易に理解するために、第１から第３の３枚のディスクを同時に装着可能なＤＶＤ記録再生装置を仮定し、鍵の生成アルゴリズムとして、第１の実施形態と同じアルゴリズムを仮定する。第１のディスクの鍵情報を、装置鍵Ａ、媒体鍵Ａ、媒体独自鍵Ａ、表題鍵Ａおよび内容鍵Ａとし、第２のディスクの鍵情報を、装置鍵Ｂ、媒体鍵Ｂ、媒体独自鍵Ｂ、表題鍵Ｂおよび内容鍵Ｂとし、第３のディスクの鍵情報を、装置鍵Ｃ、媒体鍵Ｃ、媒体独自鍵Ｃ、表題鍵Ｃおよび内容鍵Ｃとする。

本実施形態に係る著作権保護装置は、第１の実施形態と同様の方法で、第１のディスクの鍵情報を生成する。媒体鍵Ａは、装置鍵Ａで暗号化された状態で第１のディスクに記録されている。暗号化された媒体鍵Ａは、暗号化された鍵データ群ＥＫとして、鍵生成部１０に入力される。装置鍵Ａは、既に何らかの手段で鍵生成部１０に入力されている。装置鍵Ａは、例えば、予め固定的に入力されていても

よく、ある種の変換された形式で外部から供給され、鍵生成部１０で復元されることとしてもよい。鍵生成部１０は、暗号化された媒体鍵Ａを装置鍵Ａで暗号復号し、媒体鍵Ａを求める。また、鍵生成部１０には、暗号化された鍵データ群ＥＫとして、所定の値Ａ＿ａが外部から入力される。鍵生成部１０は、入力された値Ａ＿ａを用いて、媒体鍵Ａを媒体独自鍵Ａに変換する。さらに、鍵生成部１０には、暗号化された表題鍵Ａが入力される。鍵生成部１０は、暗号化された表題鍵Ａを媒体独自鍵Ａで暗号復号し、表題鍵Ａを求める。

図２と対応づけて、鍵生成手順を再度説明する。図２において、鍵生成部１０には、鍵情報ＫＩとして装置鍵Ａが入力され、暗号化された中間鍵ＥＫ１として、暗号化された媒体鍵Ａが入力される。中間鍵処理部１１は、暗号化された中間鍵ＥＫ１を鍵情報ＫＩで暗号復号し、中間鍵ＫＭである媒体鍵Ａを求める。また、鍵生成部１０には、暗号化された中間鍵情報ＥＫ１として、値Ａ＿ａが入力される。中間鍵処理部１１は、値Ａ＿ａを用いて媒体鍵Ａに対して変換を行い、新たな中間鍵ＫＭである媒体独自鍵Ａを求める。さらに鍵生成部１０には、暗号化された最終鍵ＥＫ２として、暗号化された表題鍵Ａが入力される。最終鍵処理部１２は、暗号化された表題鍵Ａを媒体独自鍵Ａで暗号復号し、最終鍵Ｋである表題鍵Ａを求める。

求めた表題鍵Ａは、最終鍵Ｋとしてコンテンツ暗号化／復号部３０に入力される。コンテンツ暗号化／復号部３０は、表題鍵Ａを用いて、暗号化処理または暗号復号処理を

行う。

第１のディスクと同様の方法で、第２および第３のディスクの鍵情報も生成される。各ディスクの鍵情報である媒体鍵Ａ、媒体独自鍵Ａ、表題鍵Ａ、媒体鍵Ｂ、媒体独自鍵Ｂ、表題鍵Ｂ、媒体鍵Ｃ、媒体独自鍵Ｃおよび表題鍵Ｃは、いずれも鍵情報保持／選択部２０に供給され、選択回路２１を経てレジスタ回路２２に記憶される。鍵情報保持／選択部２０では、外部から供給された選択情報ＳＥＬに応じて、選択回路２１が動作する。選択回路２１は、レジスタ回路２２に記憶された数種類の鍵を選択し、鍵生成部１０に出力する。例えば、第１、第２、第３の順にディスクを連続して再生した後に、再び第１のディスクを再生する場合には、第１のディスクの媒体独自鍵Ａを呼び出せばよい。

このように本実施形態に係る著作権保護装置によれば、２回目以降に鍵を生成する場合には、記憶回路からの呼び出しのみで鍵を生成できるため、短時間で鍵を生成することができる。複数のメディアを装着可能な装置において、複数のメディアに跨るランダムアクセスを行う場合には、メディアを切り替えるごとに鍵を生成する必要が生じる。したがって、このように何度も鍵生成を行う装置では、１回の鍵生成に要する時間が短縮される効果は、特に顕著となる。

図７を用いて、本実施形態に係る著作権保護装置による鍵生成時間の短縮効果を説明する。図７（ａ）は、従来の装置におけるコンテンツ再生処理時間を示す図であり、図

７（ｂ）は、本実施形態に係る装置におけるコンテンツ再生処理時間を示す図である。いずれの装置でも、第１、第２、第１、第２の順にディスクが再生され、ディスクを再生するに先立ち、ディスクの立ち上げと鍵生成とを行う必要があるとする。

従来の装置（図７（ａ））では、第２のディスクを再生した後に、第１のディスクを２回目に再生するときには、第１のディスクの鍵を生成するために、１回目に第１のディスクを再生したときと同じ時間がかかる。また、第２ディスクを再生するときも、この事情は同じである。

一方、本実施形態に係る装置（図７（ｂ））では、第１および第２のディスク用の鍵を１回目に生成するときには、従来と同じ時間がかかる。しかし、第１および第２のディスクの媒体独自鍵は、いずれも鍵情報保持／選択部２０に保持されているので、２回目以降に鍵を生成するためには、保持された媒体独自鍵を呼び出すだけ済む。したがって、２回目以降に鍵を生成するための時間は、従来の装置に比べて短縮される（図７（ｂ）の斜線部）。

なお、本実施形態では、暗号化されたコンテンツを暗号復号する場合について説明したが、逆に平文データのコンテンツを暗号化する場合でも同様の構成を採用することができる。また、鍵生成アルゴリズムは、媒体独自鍵（Ａ、Ｂ、Ｃ）と内容鍵（Ａ、Ｂ、Ｃ）とを両方とも使用しないものでもよく、片方のみ使用するものでもよい。また、表題鍵（Ａ、Ｂ、Ｃ）を生成する過程は、より複雑なものであってもよい。

また、鍵情報保持／選択部２０は、図３に示すように選択回路２１とレジスタ回路２２とを備えるものでも、図６に示すように暗号化／復号回路２３を備えるものでもよい。後者の場合の著作権保護装置は、第２および第３の実施形態を組み合わせた動作を行う。すなわち、各ディスクの鍵情報である媒体鍵Ａ、媒体独自鍵Ａ、表題鍵Ａ、媒体鍵Ｂ、媒体独自鍵Ｂ、表題鍵Ｂ、媒体鍵Ｃ、媒体独自鍵Ｃおよび表題鍵Ｃは、鍵情報保持／選択部２０の暗号化／復号回路２３によって暗号化された状態で、集積回路外部または内部の記憶回路に保持される。

この方法によれば、暗号化を行わずに集積回路内部の記憶回路に保持した場合よりも遅いが、媒体独自鍵Ａを鍵生成部１０における手順に従って生成するよりも早く、鍵を生成することができる。また、媒体独自鍵Ａは暗号化された状態で保持されるので、第１の実施形態と比べて鍵の暗号強度を高めることができる。さらに、集積回路外部の記憶回路に暗号化した鍵を保持させることができるので、保持する鍵の量が、集積回路内部の記憶回路の量に制限されることがない。また、複数のメディアを装着可能な装置において、複数のメディアに跨るランダムアクセスを行う場合には、鍵生成時間が短縮される効果は、特に顕著となる。

（第４の実施形態）

本発明の第４の実施形態に係る著作権保護装置は、鍵情報を保持することに加えて、鍵生成アルゴリズムがＣＰＲＭまたはＣＰＰＭであることを特徴とする。

装置の例として、ＤＶＤ記録再生機器を仮定する。ＤＶＤ記録再生機器は、複数の装置鍵を有する。各装置鍵には、鍵データに加えて、行列状に配置された鍵生成用データに関する行および列の情報が付与される。

ＣＰＲＭでは、暗号化された鍵データ群は、媒体鍵ブロック（Media Key Block）に格納されている。媒体鍵ブロックは、次のような種類のレコードを含んでいる。記録タイプの値が８１（１６進数）であるレコードを、検証媒体鍵レコード（Verify Media Key Record）という。記録タイプの値が０１（１６進数）であるレコードを、計算媒体鍵レコード（Calculate Media Key Record）という。記録タイプの値が８２（１６進数）であるレコードを、条件付き計算媒体鍵レコード（Conditionally Calculate Media Key Record）という。また、３２ビットの検証データDEAD BEEF（１６進数）をパターンＤＢと呼ぶ。検証媒体鍵レコードには、パターンＤＢを媒体鍵で暗号化した結果が記録されている。

図８および図９は、それぞれ、ＣＰＲＭの媒体鍵ブロックに含まれる計算媒体鍵レコード、および、条件付き計算媒体鍵レコードのデータ構造図である。図１０は、鍵情報生成および鍵情報保持の動作を示すフローチャートである。このフローチャートでは、媒体鍵が中間鍵として扱われている。なお、ＣＰＲＭおよびＣＰＰＭのアルゴリズムおよびデータ構造の詳細は、上述した第１から第４の仕様書に記載されているので、ここでは説明を省略する。

ＣＰＲＭでは、中間鍵として媒体鍵Ａと媒体独自鍵Ａと

が使用され、最終鍵として表題鍵Ａが生成される。ＣＰＰＭでは、中間鍵として媒体鍵Ａが使用され、最終鍵としてアルバム独自鍵Ａが生成される。

以下、図１０を用いて、鍵生成部１０における処理手順を説明する。

中間鍵と最終鍵とは、暗号化された状態でメディアに格納されている。鍵生成部１０は、まず変数ｎの値を１とする（ステップＳ１０１）。なお、変数Ｎは、複数の装置鍵を順に処理するために使用される変数である。複数の装置鍵を、順に装置鍵Ａ、装置鍵Ｂ、装置鍵Ｃ、…とし、各装置鍵に対応した媒体鍵を、順に媒体鍵Ａ、媒体鍵Ｂ、媒体鍵Ｃ、…とする。変数ｎが順に１、２、３、…と更新されることに対応して、装置鍵Ａ、Ｂ、Ｃ、…がアルファベット順に処理され、媒体鍵Ａ、Ｂ、Ｃ、…がアルファベット順に生成される。

次に、鍵生成部１０には、暗号化された媒体鍵Ａを復号するための装置鍵Ａが入力される（ステップＳ１０２）。なお、装置鍵Ａは、暗号化された状態で入力されることとしてもよい。この場合、鍵生成部１０は、内部で装置鍵Ａを復号する。次に、鍵生成部１０には、暗号化された媒体鍵Ａが入力される（ステップＳ１０３）。より詳細には、鍵生成部１０は、メディアに記録された媒体鍵ブロックから、装置鍵Ａに付与された行および列に対応した、暗号化された鍵情報を読み出す。次に、鍵生成部１０は、暗号化された媒体鍵Ａを装置鍵Ａで暗号復号し、媒体鍵Ａを得る（ステップＳ１０４）。ただし、ここで得られた媒体鍵は

、この時点ではまだ媒体鍵Ａと確定していないので、現媒体鍵Ａと呼ぶ。鍵生成部１０は、確定した媒体鍵Ａを得るために、さらに以下の処理を行う。

次に、鍵生成部１０は、メディアに記録された媒体鍵ブロックから検証媒体鍵レコードを読み出し、入力する（ステップＳ１０５）。次に、鍵生成部１０は、ステップＳ１０４で求めた現媒体鍵Ａを用いて、検証媒体鍵レコードを暗号復号する（ステップＳ１０６）。上述したように、検証媒体鍵レコードには、パターンＤＢを媒体鍵で暗号化した結果が記録されている。したがって、検証媒体鍵レコードを暗号復号してパターンＤＢが得られた場合には（ステップＳ１０７のＹＥＳ）、鍵生成部１０は、その時の現媒体鍵Ａを正しい媒体鍵と扱うこととし、ステップＳ１１４へ進む。

検証鍵媒体レコードを復号してもパターンＤＢが得られなった場合には（ステップＳ１０７のＮＯ）、鍵生成部１０は、メディアに格納された媒体鍵ブロックから、条件付き計算媒体鍵レコードを選出し、入力する（ステップＳ１０８）。次に、鍵生成部１０は、条件付き計算媒体レコードに含まれるバイト位置４～１１のデータ（記録データヘッダ）を現媒体鍵Ａで暗号復号する（ステップＳ１０９）。次に、鍵生成部１０は、復号結果のうちバイト位置４～７のデータがパターンＤＢであるか否か検証する（ステップＳ１１０）。復号結果がパターンＤＢではない場合には、鍵生成部１０は、ステップＳ１０８に戻る。なお、ステップＳ１１０における検証には、パターンＤＢが得られた

か否かを検証すること以外にも条件がある。その詳細は上述した第１から第４の仕様書に記載されているので、ここでは説明を省略する。

復号結果がパターンＤＢである場合には、鍵生成部１０は、復号された列情報（記録データヘッダ中のバイト位置８に記録されている）を参照し、その列情報を有する装置鍵を装置鍵Ｂとするとともに、装置鍵Ｂの行情報に対応した記録データを抽出し（ステップＳ１１１）、現媒体鍵Ａで復号する（ステップＳ１１２）。記録データは二重に暗号化されており、ステップＳ１１２ではそのうちの１つが復号されたことになる。次に、鍵生成部１０は、変数ｎに１を加え（ステップＳ１１３）、ステップＳ１０２に戻る。

ステップＳ１０２に戻った場合、鍵生成部１０は、ステップＳ１１１で求めた装置鍵について同様の処理を行う。ただし、ステップＳ１１２において、暗号化された中間鍵として、暗号化された現媒体鍵Ｂが既に入力されているので、鍵生成部１０は、２回目以降の処理ではステップＳ１０３の処理を行わない。

鍵生成部１０は、媒体鍵Ｂを解くための装置鍵Ｂを入力し（ステップＳ１０２）、暗号化された媒体鍵Ｂを装置鍵Ｂで復号し（ステップＳ１０４）、検証鍵媒体レコードを現媒体鍵Ｂで暗号復号し（ステップＳ１０６）、その結果としてパターンＤＢが得られた場合には、現媒体鍵Ｂを媒体鍵Ｂとする（ステップＳ１０７）。

ステップＳ１０７における検証結果が正しい場合には、

現媒体鍵は、正しい媒体鍵として扱われる。鍵生成部１０は、求めた媒体鍵と媒体識別子（Ｍｅｄｉａ ＩＤ）との間で演算処理を行い、媒体独自鍵（ＣＰＰＭの場合はアルバム独自鍵）を求める。鍵生成部１０は、暗号化された表題鍵を媒体独自鍵で暗号復号し、求めた表題鍵を最終鍵Ｋとしてコンテンツ暗号化／復号部３０に出力する。なお、ＣＰＰＭの場合には、鍵生成部１０は、表題鍵に代えてアルバム独自鍵を最終鍵Ｋとしてコンテンツ暗号化／復号部３０に出力する。

ステップＳ１１４以降、鍵情報保持／選択部２０が動作する。鍵情報保持／選択部２０は、変数ｎが１である場合には（ステップＳ１１４のＹＥＳ）、媒体鍵を解くための装置鍵Ａと、暗号化された媒体鍵Ａとを保持する（ステップＳ１１５）。また、鍵情報保持／選択部２０は、変数ｎが１でない場合には（ステップＳ１１４のＮＯ）、媒体鍵ｎ－１を解くためにこれまでに現れた装置鍵と、その時点で処理対象とされている暗号化された記録データと、媒体鍵を解くための装置鍵とを保持する（ステップＳ１１６）。例えば、２番目の装置鍵で正しい媒体鍵が得られた場合には、媒体鍵Ｂを得ることができたデータ、すなわち、装置鍵Ａと、装置鍵Ｂおよび媒体鍵Ｂを得ることができた二重に暗号化された鍵情報とが保持される。なお、装置鍵の使用順序は、記憶しておく必要がある。

このように本実施形態に係る著作権保護装置によれば、ＣＰＲＭやＣＰＰＭのように、行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行う

ことにより鍵を生成する場合についても、中間鍵である媒体鍵を生成できた装置鍵（暗号化された装置鍵を含む）と、暗号化された媒体鍵のデータを保持することにより、短時間で再び媒体鍵を生成することができる。

（第５の実施形態）

本発明の第５の実施形態は、複数のメディアを装着するために、各メディアごとに生成された鍵情報を保持する点で、第４の実施形態と相違する。本実施形態では、各メディアごとにそれぞれ暗号化された鍵データ群が存在する。本実施形態は、表題鍵を生成するまでの処理が第４の実施形態と相違するので、以下ではその処理について説明する。

本実施形態を容易に理解するために、第２の実施形態と同様に、第１から第３の３枚のディスクを同時に装着可能なＤＶＤ記録再生装置を仮定する。本実施形態に係る著作権保護装置は、第４の実施形態と同様に、第１のディスクの鍵情報を生成する。

第１のディスクには、中間鍵と最終鍵とが、暗号化された状態で記録されている。鍵生成部１０には、暗号化された媒体鍵Ａ＿１を復号するための装置鍵Ａ＿１が入力される（ステップＳ１０２）。なお、装置鍵Ａ＿１は、暗号化された状態で入力されることとしてもよい。この場合、鍵生成部１０は、内部で装置鍵Ａ＿１を復号する。次に、鍵生成部１０には、暗号化された媒体鍵Ａ＿１が入力される（ステップＳ１０３）。より詳細には、鍵生成部１０は、メディアに記録された媒体鍵ブロックから、装置鍵Ａ＿１

に付与された行および列に対応した、暗号化された鍵情報を読み出す。次に、鍵生成部１０は、暗号化された媒体鍵Ａ＿１を装置鍵Ａ＿１で暗号復号し、媒体鍵Ａ＿１を得る（ステップＳ１０４）。ただし、ここで得られた媒体鍵は、この時点ではまだ媒体鍵Ａ＿１と確定していないので、現媒体鍵Ａ＿１と呼ぶ。鍵生成部１０は、確定した媒体鍵Ａ＿１を得るために、さらに以下の処理を行う。

次に、鍵生成部１０は、メディアに記録された媒体鍵ブロックから検証鍵媒体レコードを読み出し、入力する（ステップＳ１０５）。次に、鍵生成部１０は、ステップＳ１０４で求めた現媒体鍵Ａ＿１を用いて、検証鍵媒体レコードを暗号復号する（ステップＳ１０６）。上述したように、検証鍵媒体レコードには、パターンＤＢを媒体鍵で暗号化した結果が記録されている。したがって、検証鍵媒体レコードを暗号復号してパターンＤＢが得られた場合には（ステップＳ１０７のＹＥＳ）、鍵生成部１０は、その時の現媒体鍵Ａ＿１を正しい媒体鍵と扱うこととし、ステップＳ１１４へ進む。

検証媒体レコードを復号してもパターンＤＢが得られなかった場合には（ステップＳ１０７のＮＯ）、鍵生成部１０は、メディアに格納された媒体鍵ブロックから、条件付き計算媒体鍵レコードを選出し、入力する（ステップＳ１０８）。次に、鍵生成部１０は、条件付き計算媒体レコードに含まれるバイト位置４～１１のデータ（記録データヘッダ）を現媒体鍵Ａ＿１で復号する（ステップＳ１０９）。次に、鍵生成部１０は、復号結果のうちバイト位置４～

７のデータがパターンＤＢであるか否か検証する（ステップＳ１１０）。復号結果がパターンＤＢではない場合には、鍵生成部１０は、ステップＳ１０８に戻る。なお、ステップＳ１１０における検証には、パターンＤＢが得られたか否かを検証すること以外にも条件がある。その詳細は上述した第１から第４の仕様書に記載されているので、ここでは説明を省略する。

復号結果がパターンＤＢである場合には、鍵生成部１０は、復号された列情報（記録データヘッダ中のバイト位置８に記録されている）を参照し、その列情報を有する装置鍵を装置鍵Ａ＿２とするとともに、装置鍵Ａ＿２の行情報に対応した記録データを抽出し（ステップＳ１１１）、現媒体鍵Ａ＿１で復号する（ステップＳ１１２）。記録データは二重に暗号化されており、ステップＳ１１２ではそのうちの１つが復号されたことになる。次に、鍵生成部１０は、変数ｎに１を加え（ステップＳ１１３）、ステップＳ１０２に戻る。

ステップＳ１０２に戻った場合、鍵生成部１０は、ステップＳ１１１で求めた装置鍵について同様の処理を行う。ただし、ステップＳ１１２において、暗号化された中間鍵として、暗号化された現媒体鍵Ａ＿２が既に入力されているので、鍵生成部１０は、２回目以降の処理ではステップＳ１０３の処理を行わない。

鍵生成部１０は、媒体鍵Ａ＿２を解くための装置鍵Ａ＿２を入力し（ステップＳ１０２）、暗号化された媒体鍵Ａ＿２を装置鍵Ａ＿２で復号し（ステップＳ１０４）、検証

媒体鍵レコードを現媒体鍵Ａ＿２で復号し（ステップＳ１０６）、その結果としてパターンＤＢが得られた場合には、現媒体鍵Ａ＿２を媒体鍵Ａ＿２とする（ステップＳ１０７）。

ステップＳ１０７における検証結果が正しい場合には、現媒体鍵は、正しい媒体鍵として扱われる。鍵生成部１０は、求めた媒体鍵と媒体識別子との間で演算処理を行い、媒体独自鍵（ＣＰＰＭの場合はアルバム独自鍵）を求める。鍵生成部１０は、暗号化された表題鍵を媒体独自鍵で暗号復号し、求めた表題鍵を最終鍵Ｋとしてコンテンツ暗号化／復号部３０に出力する。なお、ＣＰＰＭの場合には、鍵生成部１０は、表題鍵に代えてアルバム独自鍵を最終鍵Ｋとして、コンテンツ暗号化／復号部３０に出力する。

ステップＳ１１４以降、鍵情報保持／選択部２０が動作する。鍵情報保持／選択部２０は、変数ｎが１である場合には（ステップＳ１１４のＹＥＳ）、媒体鍵を解くための装置鍵Ａ＿１と、暗号化された媒体鍵Ａ＿１とを保持する（ステップＳ１１５）。また、鍵情報保持／選択部２０は、変数ｎが１でない場合には（ステップＳ１１４のＮＯ）、媒体鍵ｎ－１を解くためにこれまでに現れた装置鍵と、その時点で処理対象とされている暗号化された記録データと、媒体鍵を解くための装置鍵とを保持する（ステップＳ１１６）。例えば、２番目の装置鍵で正しい媒体鍵が得られた場合には、媒体鍵Ａ＿２を得ることができたデータ、すなわち、装置鍵Ａ＿１と、装置鍵Ａ＿２と媒体鍵Ａ＿２を得ることができた二重に暗号化された鍵情報とが保持さ

れる。なお、装置鍵の使用順序は、記憶しておく必要がある。

第１のディスクと同様の方法で、第２および第３のディスクの鍵情報も生成され、鍵情報保持／選択部２０に保持される。なお、ステップＳ１１４に処理が到達した時点における変数ｎの値はディスクごとに異なるため、保持すべき情報の個数および種類はディスクごとに異なることは、言うまでもない。例えば、第２のディスクについては、装置鍵Ｂ＿１と、装置鍵Ｂ＿２および媒体鍵Ｂ＿２を得ることができた二重に暗号化された鍵情報とが保持され、第３のディスクについては、装置鍵Ｃ＿１と、装置鍵Ｃ＿２と、装置鍵Ｃ＿３および媒体鍵Ｃ＿３を得ることができた二重に暗号化された鍵情報とが保持される場合がありうる。

このように本実施形態に係る著作権保護装置によれば、ＣＰＲＭやＣＰＰＭのように、行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより鍵を生成する場合であって、複数のディスクを装着可能に構成されている場合についても、各ディスクの中間鍵である媒体鍵を生成できた装置鍵（暗号化された装置鍵を含む）と、暗号化された媒体鍵のデータを保持することにより、短時間で再び媒体鍵を作成できる。

この効果は、ディスクに跨るランダムアクセスを行う場合に特に顕著となる。例えば、第１、第２、第３、第２、第１、第３の順にディスクを連続して再生する場合に、上述した鍵情報を保持していなければ、ディスクを切り替えるごとに始めから鍵生成手順を行う必要が生じる。これに

対して、本実施形態のように正しい媒体鍵を生成するために必要な装置鍵と、暗号化された鍵情報とを保持していれば、保持した情報を呼び出すだけで、短時間で鍵を生成することができる。この効果は、第３の実施形態と同様であり、図７を用いて既に説明したとおりである。しかも、必要な鍵情報は暗号化された状態で保持されるので、暗号強度の点でも充分な能力を有する。

（第６の実施形態）

本発明の第６の実施形態は、各ディスクについて生成した中間鍵を、第５の実施形態と異なる方式で保持することを特徴とする。第１の方式を採用した場合、著作権保護装置は、生成した媒体鍵を暗号化／復号回路２３で暗号化して出力する。第２の方式を採用した場合、著作権保護装置は、生成した媒体鍵を集積回路内部に保持する。第３の方式を採用した場合、著作権保護装置は、生成した媒体独自鍵（ＣＰＰＭの場合はアルバム独自鍵）を暗号化／復号回路２３で暗号化して出力する。第４の方式を採用した場合、著作権保護装置は、生成した媒体独自鍵（ＣＰＰＭの場合はアルバム独自鍵）を集積回路内部に保持する。

図１１は、第１の方式を採用した場合の鍵情報生成および鍵情報保持の動作を示すフローチャートである。図１１は、ステップＳ１２１のみが図１０と相違する。図１２は、第４の方式を採用した場合の鍵情報生成および鍵情報保持の動作を示すフローチャートである。図１２は、ステップＳ１３１のみが図１０と相違する。各フローチャートにおける処理は、第５の実施形態と同様であるので、ここで

は説明を省略する。

このように本実施形態に係る著作権保護装置によれば、ＣＰＲＭやＣＰＰＭのように、行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより鍵を生成する場合であって、複数のディスクを装着可能に構成されている場合についても、各ディスクの中間鍵である媒体鍵を生成できる装置鍵（暗号化された装置鍵を含む）と、暗号化された媒体鍵のデータを保持することにより、短時間で再び媒体鍵を作成することができる。したがって、ディスクに跨るランダムアクセスを行う場合に、例えば、第１、第２、第３、第２、第１、第３の順にディスクを連続して再生する場合に、非常に有効である。なお、複数のディスクが装着されていない場合にも、同様の効果を奏することは言うまでもない。

（第７の実施形態）

本発明の第７の実施形態は、出力切り替えスイッチを用いて、鍵生成中の出力制御を行うことを特徴とする。図１３は、本実施形態に係る著作権保護装置のうち、鍵生成部１０とコンテンツ暗号化／復号部３０と出力切り替えスイッチ３７とを示した図である。図１３は、図４と対比して描かれている。

第１の実施形態では、コンテンツ暗号化／復号部３０が、鍵生成期間通知信号ＧＥＮがアクティブである間は、暗号処理を行った結果の出力データＤＯを出力しないこととした。本実施形態では、出力切り替えスイッチ３７が、出力データＤＯを制御する。

具体的に言うと、出力切り替えスイッチ３７には、鍵生成部１０から出力された鍵生成期間通知信号ＧＥＮが入力される。信号ＧＥＮが非アクティブ（鍵生成中でない）である場合、出力切り替えスイッチ３７は、コンテンツ暗号化／復号部３０からの出力信号（図１３のａ）を選択して出力する。これに対して、信号ＧＥＮがアクティブ（鍵生成中）である場合、出力切り替えスイッチ３７は、コンテンツ暗号化／復号部３０への入力信号（図１３のｂ）を選択して出力する。

図１４は、本実施形態に係る著作権保護装置の入力信号のタイミングチャートである。図１４において、コンテンツ暗号化／復号部３０の入力信号は、Ｄ０、Ｄ１、Ｄ２、…であり、コンテンツ暗号化／復号部３０の出力信号は、ｄ０、ｄ１、ｄ２、…である。鍵生成期間通知信号ＧＥＮは、鍵生成中にＨレベルになるとする。

出力切り替えスイッチ３７は、信号ＧＥＮが非アクティブである場合、コンテンツ暗号化／復号部３０の出力信号を選択して出力する。したがって、著作権保護装置からはｄ７、ｄ８、ｄ９、…等のデータが出力される。これに対して、信号ＧＥＮがアクティブである場合、出力切り替えスイッチ３７は、コンテンツ暗号化／復号部３０の入力信号を選択し、そのまま出力する。したがって、著作権保護装置からはＤ０からＤ７までのデータが出力される。

このように本実施形態に係る著作権保護装置によれば、誤った鍵で暗号化または暗号復号を行った結果を出力しないので、次段の処理手段に悪影響を及ぼすことがない。

（第８の実施形態）

本発明の第８の実施形態は、鍵生成中はデータ入力を禁止することを特徴とする。図１５は、本実施形態に係る著作権保護装置のうち、鍵生成部１０とコンテンツ暗号化／復号部３１とを示した図である。図１５は、図４と対比して描かれている。

鍵生成部１０は、第１の実施形態と同様に、最終鍵Ｋとして表題鍵Ａをコンテンツ暗号化／復号部３１に出力する。コンテンツ暗号化／復号部３１には、表題鍵Ａと入力データＤＩとが入力される。コンテンツ暗号化／復号部３１は、第１の実施形態と同様に、入力データＤＩを表題鍵Ａで暗号化または暗号復号し、その結果として出力データＤＯを出力する。

鍵生成部１０は、装置鍵Ａや媒体鍵Ａ等の中間鍵の生成を開始してから、媒体独自鍵Ａ等の中間鍵または表題鍵Ａ等の最終鍵を生成し終えるまでの間、鍵生成期間通知信号ＧＥＮをアクティブにしてコンテンツ暗号化／復号部３１に出力する。コンテンツ暗号化／復号部３１は、信号ＧＥＮがアクティブ（鍵生成中）である場合、データの入力を停止させるため、入力許可信号ＩＥを非アクティブ（入力禁止状態）にして出力する。これに対して、信号ＧＥＮが非アクティブ（鍵生成中でない）である場合、コンテンツ暗号化／復号部３１は、自らが入力データＤＩを受け入れ可能か否かを判断し、受け入れ可能であれば、入力許可信号をアクティブ（入力許可状態）にして出力し、受け入れ不可能であれば、入力許可信号ＩＥを非アクティブにして

出力する。

図１６は、本実施形態に係る著作権保護装置の入力信号のタイミングチャートである。図１６において、鍵生成期間通知信号ＧＥＮは、鍵生成中にＨレベルとなり、入力許可信号ＩＥは、入力許可状態のときにＨレベルとなるものとする。

信号ＧＥＮがアクティブに変化すると同時に、コンテンツ暗号化／復号部３１は、入力許可信号ＩＥを非アクティブに切り替える。このため鍵生成中は、コンテンツ暗号化／復号部３１に新たなデータが入力されることはない。データ入力が停止するため、コンテンツ暗号化／復号部３１は、この期間データを出力しない。

その後、信号ＧＥＮが非アクティブに変化すると、コンテンツ暗号化／復号部３１は、入力許可信号ＩＥをアクティブに切り替える。このため、データ入力が再開される。図１６について言えば、データ入力が再開されて、Ｄ０、Ｄ１、Ｄ２、…等のデータが入力されると、ｄ０、ｄ１、ｄ２、…等のデータが出力される。

このように本実施形態に係る著作権保護装置によれば、鍵生成中はデータ入力を禁止するので、鍵生成中にデータが入力されることがない。したがって、鍵生成中に誤ったデータを出力しないという効果を奏する。

なお、本実施形態では、コンテンツ暗号化／復号部３１が入力許可信号ＩＥを出力することとしたが、図１７に示すように、鍵生成部１３が入力許可信号ＩＥを出力することとしてもよい。このような変形例によっても、第８の実

施形態と同様の効果を奏する。

なお、著作権保護装置の他の構成要素から他の入力許可信号が出力される場合には、この信号と、コンテンツ暗号化／復号部または鍵生成部から出力された入力許可信号との間で論理演算を行い、外部に出力する入力許可信号を求めることは言うまでもない。

（第９の実施形態）

図１８は、本発明の第９の実施形態に係る著作権保護装置のうち、コンテンツ暗号化／復号部３２、入力用レジスタ４０、入力許可信号生成回路６１、レジスタ６２、論理和回路６３を示した図である。入力用レジスタ４０は、第１から第６のレジスタ４１～４６を含んでいる。図１８は、図５と対比して描かれている。

第１の実施形態では、定期的にリセットを行い、異常状態に陥っても正しいデータが入力されたときには正しく動作することを目的とした。本実施形態は、入力許可信号が非アクティブ（入力禁止状態）になった後にデータが入力されても、入力許可信号が非アクティブになった後に入力されたデータ（以下、「過剰データ」という）を欠落させることなく、首尾良く処理することを目的とする。

本実施形態を容易に理解するために、コンテンツ暗号化／復号部３２には、データは１バイト単位で入力され、入力許可信号ＩＥが非アクティブになった後に、１バイトの過剰データが入力されると仮定する。入力データは、第１から第６のレジスタ４１～４６に順次保持される。コンテンツ暗号化／復号部３２には、第３から第６のレジスタ４

３～４６から出力された４バイト分のデータが、同時に入力される。コンテンツ暗号化／復号部３２は、入力されたデータに所定の処理を行い、その結果を出力する。また、コンテンツ暗号化／復号部３２は、内部処理でオーバーフローが発生することを検知し、オーバーフローが発生する一つ前のクロックサイクルで、オーバーフローの発生を示す通知信号ＶＦを出力する。

コンテンツ暗号化／復号部３２におけるオーバーフロー発生の具体的な状況やオーバーフローの検知方法は、本発明の特徴ではないが、例えば以下の場合にオーバーフローが起こりうる。すなわち、コンテンツ暗号化／復号部３２は、入力信号をレジスタに保持し一定速度で演算処理を行うが、データの入力速度が可変である場合には、データの入力速度がコンテンツ暗号化／復号部３１の処理速度を超える場合がある。このような場合に、コンテンツ暗号化／復号部３１のレジスタでオーバーフローが発生する。

オーバーフロー通知信号ＶＦは、入力許可信号生成回路６１に入力される。入力許可信号生成回路６１は、信号ＶＦを受け取ると、入力許可信号ＩＥを非アクディブ（入力禁止状態）にして出力する。入力許可信号ＩＥが非アクティブに変化すると、データ入力は停止されるが、先に仮定したように、１バイトの過剰データが入力される。

第１から第６のレジスタ４１～４６は、いずれも、ロード信号ＬＤで制御される。ロード信号ＬＤは、図１８に示すように、入力許可信号ＩＥと、信号ＩＥをレジスタ６２で１クロックサイクル遅延させた信号とを、論理和回路６

３で論理和して求めた信号である。ロード信号ＬＤは、入力許可信号ＩＥよりも１クロックサイクル分長くアクティブとなる。このため、第１から第６のレジスタ４１～４６は、入力許可信号ＩＥが非アクティブになった後、さらに１バイト入力データＤＩをロードする。よって、入力許可信号ＩＥが非アクティブとなった後に入力された１バイトの過剰データは、第１のレジスタ４１にロードされる。

図１９は、本実施形態に係る著作権保護装置の入力信号のタイミングチャートである。図１９において、コンテンツ暗号化／復号部３１は、時刻Ｔａで内部処理がオーバーフローすることを検知し、その１クロックサイクル後の時刻Ｔｂで入力許可信号ＩＥを非アクティブにして出力する。時刻Ｔｂではデータ７が入力されるので、著作権保護装置は、これを取り込む必要がある。時刻Ｔｂではロード信号ＬＤはアクティブであるため、データＤ７は、第１のレジスタ４１に首尾よく取り込まれる。

入力許可信号ＩＥは時刻Ｔｂで非アクティブに変化するが、１バイトの過剰データＤ８が入力される。時刻Ｔｃでもロード信号ＬＤはまだアクティブであるため、データＤ８は、第１のレジスタ４１に首尾良く取り込まれる。その後、コンテンツ暗号化／復号部３１のオーバーフロー状態が解消され、時刻Ｔｄで入力許可信号ＩＥがアクティブに変化すると、時刻Ｔｄ以降、Ｄ９、Ｄ１０、Ｄ１１…等のデータが入力される。これらのデータも、第１のレジスタ４１に順に取り込まれる。

図１９に示すように、入力許可信号ＩＥが途中で非アク

ティブになり、入力許可信号ＩＥが非アクティブに変化した後に１バイトの過剰データが入力される場合でも、コンテンツ暗号化／復号部３２に入力される第３から第６のレジスタ４３～４６の出力信号には、データの欠落が生じない。したがって、コンテンツ暗号化／復号部３２は、欠落なく入力されたデータを正しく処理することができる。

このように本実施形態に係る著作権保護装置によれば、入力許可信号が非アクティブになった後にデータが入力される場合でも、過剰データを欠落させることなく、首尾良く処理することができる。

なお、本実施形態では、１バイト単位でデータが入力され、１バイトの過剰データが入力されると仮定したが、入力データの単位と過剰データの個数とは任意でよい。過剰データの個数が２以上である場合には、過剰データの個数に応じて、入力用レジスタの段数と入力許可信号ＩＥを引き延ばす期間とを調整すればよい。

（第１０の実施形態）

図２０は、本発明の第１０の実施形態に係る著作権保護装置のうち、コンテンツ暗号化／復号部３３、入力用レジスタ４０、先頭パターン検出器５０、レジスタ６２、論理和回路６３、リセット／入力許可信号生成回路６４、Ｒ／Ｗ制御回路７１、および、レジスタ７２を示した図である。入力用レジスタ４０は、第１から第６のレジスタ４１～４６を含んでいる。図２０は、図５と対比して描かれている。

本実施形態は、図５で示したコンテンツ暗号化／復号部

３０、または、図１８で示したコンテンツ暗号化／復号部３２とを、Ｒ／Ｗ制御回路７１とレジスタ７２とコンテンツ暗号化／復号部３３とに詳細化したものである。第９の実施形態では、入力許可信号ＩＥがアクティブであるときは、第３から第６のレジスタ４３～４６に蓄積されたデータが出力されていた。本実施形態は、入力許可信号ＩＥがアクティブであることを、Ｒ／Ｗ制御回路７１における書き込み許可の条件に追加したことを特徴とする。

本実施形態を容易に理解するために、図２０に示す著作権保護装置には、第１の実施形態と同様に、データは８ビット並列に２０４８バイトを一単位として入力されると仮定する。また、一単位のデータの先頭には３２ビットの先頭パターンＰが配置されると仮定する。

図２０に示す著作権保護装置には、２０４８バイトで一単位となる入力データＤＩが、１バイトづつ順次入力される。入力されたデータは、第１から第６のレジスタ４１～４６に順次保持される。第３から第６のレジスタ４３～４６の出力は、Ｒ／Ｗ制御回路７１からの制御に従ってレジスタ７２に書き込まれる。Ｒ／Ｗ制御回路７１は、レジスタ７２に書き込み可能な領域が存在すれば、レジスタ７２への書き込みを許可する。また、Ｒ／Ｗ制御回路７１は、レジスタ７２にまだ読み出されていないデータが存在していれば、そのデータをレジスタ７２から読み出し、コンテンツ暗号化／復号部３３に出力する。さらに、Ｒ／Ｗ制御回路７１は、レジスタ７２内のまだ読み出されていないデータ領域に対する書き込みを禁止し、書き込み禁止である

旨を示す書き込み禁止通知信号ＷＸを出力する。加えて、Ｒ／Ｗ制御回路７１は、レジスタ７２に読み出されていないデータが存在する旨を示す未読み出しデータ残留通知信号ＲＥＭを出力する。通知信号ＷＸおよびＲＥＭは、リセット／入力許可信号生成回路６４に入力される。

レジスタ７２からの出力は、コンテンツ暗号化／復号部３３に入力される。コンテンツ暗号化／復号部３３は、入力されたデータに対して所定の処理を行い、その結果を出力する。また、コンテンツ暗号化／復号部３２は、内部処理がオーバーフローしたときには、読み出し停止信号ＲＸを出力する。さらに、コンテンツ暗号化／復号部３２は、内部に処理中のデータが残留していない旨を示す処理完了信号ＤＮを出力する。読み出し停止信号ＲＸはＲ／Ｗ制御回路７１に入力され、処理完了信号ＤＮはリセット／入力許可信号生成回路６４に入力される。

リセット／入力許可信号生成回路６４は、書き込み禁止通知信号ＷＸを受けたときには、直ちに入力許可信号ＩＥを非アクティブ（入力禁止状態）にして出力し、データ入力を停止させる。入力許可信号ＩＥが非アクティブになった後の動作は第９の実施形態と同じであるので、ここでは説明を省略する。

先頭パターン検出器５０は、第１から第４のレジスタ４１～４４に蓄積されたデータを監視し、先頭パターンＰを検出した旨を示す検出信号ＤＥＴを出力する。検出信号ＤＥＴは、リセット／入力許可信号生成回路６４に入力される。

リセット／入力許可信号生成回路６４は、通知信号ＲＥＭが「未処理データなし」を示し、かつ、処理完了信号ＤＮが処理完了を示している状態で、検出信号ＤＥＴを受けたときには、Ｒ／Ｗ制御回路７１とコンテンツ暗号化／復号部３３にリセット信号ＲＳＴを出力する。

これに対して、リセット／入力許可信号生成回路６４は、通知信号ＲＥＭが「未処理データあり」を示すか、または、処理完了信号ＤＮが処理未完了を示している状態で、検出信号ＤＥＴを受けたときには、入力許可信号ＩＥを非アクティブにして出力し、データ入力を停止させるとともに、リセット待機状態に遷移する。本実施形態におけるリセット待機の意味と動作は、第１の実施形態と同じである。

リセット／入力許可信号生成回路６４は、リセット待機状態で、通知信号ＲＥＭが「未処理データなし」となり、かつ、処理完了信号ＤＮが処理完了となったときに、Ｒ／Ｗ制御回路７１とコンテンツ暗号化／復号部３２とにリセット信号ＲＳＴを出力し、リセット待機状態を解除する。リセット／入力許可信号生成回路６４は、このとき同時に入力許可信号ＩＥをアクティブ（入力許可状態）にして出力する。

このように本実施形態に係る著作権保護装置によれば、定期的にリセットを正しく行うことができ、異常状態に陥っても、正しいデータが入力すれば正しく動作し、かつ、入力許可信号が非アクティブになった後にデータが入力される場合でも、過剰データを欠落させることなく、首尾良

く処理することができる。

なお、本実施形態についても、第１の実施形態と同様に、先頭パターンの長さや値は任意である。また、本実施形態では１バイトの過剰データが入力されると仮定したが、過剰データの個数は任意である。過剰データの個数が２以上である場合には、過剰データの個数に応じて、入力用レジスタの段数と入力許可信号ＩＥを引き延ばす期間とを調整すればよい。

（第１１の実施形態）

本発明の第１１の実施形態は、入力許可信号が非アクティブになった後のデータの処理を、ＦＩＦＯ（First In First Out）形式のメモリ、または、同様のアドレス制御を行うメモリを用いて行うことを特徴とする。

図２１は、本実施形態に係る著作権保護装置のうち、入力許可信号生成回路６５、Ｒ／Ｗ制御回路７３、メモリ７４、および、コンテンツ暗号化／復号部３４を示した図である。

本実施形態を容易に理解するために、コンテンツ暗号化／復号部３４にはデータは４バイト並列に入力され、入力許可信号ＩＥが非アクティブ（入力禁止状態）になった後に、４バイトの過剰データが入力されると仮定する。

メモリ７４には、入力データＤＩが順次入力される。コンテンツ暗号化／復号部３４は、メモリ７４を経由して入力されたデータに所定の処理を行い、出力データＤＯを出力する。コンテンツ暗号化／復号部３４は、内部処理がオーバーフロー状態となる１つ前のクロックサイクルで、デ

ータを受け入れ可能か否かを示す通知信号ＡＫを非アクティブ（受け入れ不可）にして出力する。

メモリ７４に対する読み出しおよび書き込み制御は、Ｒ／Ｗ制御回路７３によって行われる。Ｒ／Ｗ制御回路７３は、入力データＤＩが入力されれば、データ書き込みを許可する。また、Ｒ／Ｗ制御回路７３は、メモリ７４に読み出し可能なデータが存在し、かつ、通知信号ＡＫが「受け入れ可能」を示す場合には、メモリ７４からデータを読み出し、コンテンツ暗号化／復号部３４に供給する。さらに、Ｒ／Ｗ制御回路７３は、メモリ７４についての読み出しアドレスＲＡと書き込みアドレスＷＡとを入力許可信号生成回路６５に出力する。

入力許可信号生成回路６５は、読み出しアドレスＲＡと書き込みアドレスＷＡとの差が２となれば、入力許可信号ＩＥを非アクティブ（入力禁止状態）にして出力し、データ入力を停止させる。入力許可信号ＩＥが非アクティブになった後には、４バイトの過剰データが入力されるが、メモリ７４のデータ幅は４バイトである。このため、過剰データをメモリ７４に書き込んでも、読み出しアドレスＲＡと書き込みアドレスＷＡとが同じ値にはならず、未読み出しデータが上書きされることはない。

読み出しアドレスＲＡが更新され、読み出しアドレスＲＡと書き込みアドレスＷＡとの差が２を超えた時に、入力許可信号生成回路６５は、入力許可信号ＩＥをアクティブ（入力許可状態）にして出力する。これにより、入力許可信号ＩＥが非アクティブになった後に入力された４バイト

の過剰データを欠落させることなく、首尾良く処理することができる。

このように、本実施形態に係る著作権保護装置によれば、第１０の実施形態と同様に、入力許可信号が非アクティブになった後にデータが入力される場合でも、過剰データを欠落させることなく、首尾良く処理することができる。

なお、本実施形態における入力データの一単位のサイズ等は、他の実施形態と同様に、仮定した以外のパラメータでもよいことは言うまでもない。

また、第１０および第１１の実施形態を組み合わせることにより、図２２に示すような著作権保護装置が得られる。図２２に示す回路の動作は、第１０および第１１の実施形態と同様であるので、ここでは説明を省略するが、この装置は、入力許可信号ＩＥが非アクティブとなった後に入力される過剰データを２バイトまで取り込むことができる。

産業上の利用可能性

以上のように、本発明に係る著作権保護装置は、第１に暗号化または暗号復号する際に使用される鍵の生成時間を短縮し、第２に鍵生成中は不要なデータを出力せず、第３に異常状態に陥っても所定のパターンが入力されると正しい状態に復帰し、また、入力許可信号が非アクティブとなった後に入力された過剰データを首尾良く処理することができる。

請求の範囲

1．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、

前記鍵を生成するための中間鍵および前記鍵の少なくとも一方を、鍵として認識できない形式で保持する保持手段とを備えた、著作権保護装置。

2．　前記鍵生成手段は、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理手段は、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行うことを特徴とする、請求項1に記載の著作権保護装置。

3．　前記保持手段は、前記中間鍵および前記鍵を集積回路内の記憶回路に保持することを特徴とする、請求項1に記載の著作権保護装置。

4．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、

前記鍵を生成するための中間鍵および前記鍵の少なくと

も一方を、暗号化して保持する保持手段とを備えた、著作権保護装置。

5．　前記鍵生成手段は、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理手段は、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行うことを特徴とする、請求項4に記載の著作権保護装置。

6．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより、コンテンツに暗号処理を行うための鍵と、前記鍵を生成するための中間鍵とを生成する鍵生成手段と、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、

前記中間鍵および前記鍵生成用データの少なくとも一方を保持する保持手段とを備えた、著作権保護装置。

7．　前記鍵生成手段は、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理手段は、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持手段は、前記中間鍵および前記鍵生成用データを各メディアごとに保持することを特徴とする、請求項6に記載の著作権保護装置。

8．　コンテンツの暗号化または暗号復号を行う著作権保護方法であって、

コンテンツに暗号処理を行うための鍵を生成する鍵生成ステップと、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、

前記鍵を生成するための中間鍵および前記鍵の少なくとも一方を、鍵として認識できない形式で保持する保持ステップとを備えた、著作権保護方法。

9. 前記鍵生成ステップは、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理ステップは、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行うことを特徴とする、請求項8に記載の著作権保護方法。

10. コンテンツの暗号化または暗号復号を行う著作権保護方法であって、

コンテンツに暗号処理を行うための鍵を生成する鍵生成ステップと、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、

前記鍵を生成するための中間鍵および前記鍵の少なくとも一方を、暗号化して保持する保持ステップとを備えた、著作権保護方法。

11. コンテンツの暗号化または暗号復号を行う著作権保護方法であって、

行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより、コンテンツに暗号処理を行うための鍵と、前記鍵を生成するための中間鍵

とを生成する鍵生成テップと、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、

前記中間鍵および前記鍵生成用データの少なくとも一方を保持する保持ステップとを備えた、著作権保護方法。

１２．　前記鍵生成ステップは、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理ステップは、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持ステップは、前記中間鍵および前記鍵生成用データを各メディアごとに保持することを特徴とする、請求項１１に記載の著作権保護方法。

１３．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段と、

暗号処理を行うか否かを示す識別情報を含んだコンテンツが入力され、前記識別情報に従って前記鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段とを備え、

前記暗号処理手段は、前記通知信号が鍵生成中を示す場合は、前記暗号処理結果の出力を抑制することを特徴とする、著作権保護装置。

１４．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段と、

暗号処理を行うか否かを示す識別信号を含んだコンテンツが入力され、前記識別信号に従って前記鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段と、

前記通知信号が鍵生成中を示す場合は、前記暗号処理手段に入力されたコンテンツを選択し、それ以外の場合は、前記暗号処理手段から出力された暗号処理結果を選択して出力する選択手段とを備えた、著作権保護装置。

１５．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段と、

暗号処理を行うか否かを示す識別信号を含んだコンテンツが入力され、前記識別信号に従って前記鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段とを備え、

前記暗号処理手段は、前記通知信号が鍵生成中を示す場合は、コンテンツの入力を制御する入力許可信号を入力禁止状態に切り替えることを特徴とする、著作権保護装置。

１６．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成する鍵生成

手段と、

暗号処理を行うか否かを示す識別信号を含んだコンテンツが入力され、前記識別信号に従って前記鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段とを備え、

前記鍵生成手段は、鍵生成中は、コンテンツの入力を制御する入力許可信号を入力禁止状態に切り替えることを特徴とする、著作権保護装置。

１７．　複数のシンボルごとに処理単位の先頭を示す先頭パターンを含んだ入力信号を処理する信号処理装置であって、

順次入力された前記入力信号を保持するレジスタと、

前記レジスタに保持された入力信号に、前記先頭パターンが含まれていることを検出する先頭パターン検出手段と、

前記レジスタを経由して供給された前記入力信号に所定の信号処理を行うとともに、前記入力信号を処理中か否かを通知する信号処理手段と、

前記先頭パターン検出手段が前記先頭パターンを検出したときに前記信号処理手段が処理中でない場合には、リセット信号を前記信号処理手段に出力し、前記先頭パターン検出手段が前記先頭パターンを検出したときに前記信号処理手段が処理中である場合には、入力を制御する入力許可信号を入力禁止状態に切り替えるとともにリセット待機状態に遷移し、リセット待機状態で前記信号処理手段における処理が完了したときに、リセット信号を前記信号処理手

段に出力する制御信号生成手段とを備えた、信号処理装置。

１８．　入力許可信号に従ってシンボルごとに入力される入力信号を処理する信号処理装置であって、

前記入力許可信号が入力禁止状態に変化した後に高々ｃシンボル分の前記入力信号が入力され、前記入力信号を一度にｂシンボル分処理するとともに、内部処理のオーバーフロー状態を通知する信号処理手段と、

前記信号処理手段における処理がオーバーフロー状態となったときに、前記入力許可信号を入力禁止状態に切り替える入力許可信号生成手段と、

ａシンボル分の前記入力信号を保持し、前記入力許可信号が入力許可状態であるときにはｂシンボルを前記信号処理手段に出力し、前記ａと前記ｂと前記ｃとにはａ≧（ｂ＋ｃ）なる関係が成立し、前記入力許可信号と当該信号を１クロックサイクル遅延させた信号との論理和信号をロード信号として用いるレジスタとを備えた、信号処理装置。

１９．　入力許可信号に従ってシンボルごとに入力される入力信号を処理する信号処理装置であって、

前記入力許可信号が入力禁止状態に変化した後に高々ｃシンボル分の前記入力信号が入力され、前記入力信号に所定の処理を行うとともに、前記入力信号を受け入れ可能か否かを通知する信号処理手段と、

前記入力信号を記憶し、記憶した前記入力信号を前記信号処理手段に対して出力するメモリと、

前記信号処理手段が前記入力信号を受け入れ可能である

場合には、データが読み出されるように前記メモリを制御し、未だ読み出されていないデータには上書きしないように書き込み制御を行いながら、書き込みアドレスと読み出しアドレスとを出力するメモリ制御手段と、

前記メモリ制御手段から出力された書き込みアドレスと読み出しアドレスとに基づき算出した書き込み余裕量が少なくともｃシンボルになったときに、前記入力許可信号を入力禁止状態に切り替える入力許可信号生成手段とを備えた、信号処理装置。

補正書の請求の範囲

[２００１年１１月２６日（２６．１１．０１）国際事務局受理：出願当初の請求の範囲１－２，４－５及び８－１０は補正された；他の請求の範囲は変更なし。（４頁）]

１．　（補正後）コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

メディアおよび前記メディアの記録再生装置に蓄積された鍵情報を用いて中間鍵を生成し、前記中間鍵を用いて、コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、

前記中間鍵を鍵として認識できない形式で保持する保持手段とを備えた、著作権保護装置。

２．　（補正後）前記鍵生成手段は、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理手段は、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持手段は、複数のメディアについて生成された前記中間鍵を、鍵として認識できない形式で保持することを特徴とする、請求項１に記載の著作権保護装置。

３．　前記保持手段は、前記中間鍵および前記鍵を集積回路内の記憶回路に保持することを特徴とする、請求項１に記載の著作権保護装置。

４．　（補正後）コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

メディアおよび前記メディアの記録再生装置に蓄積された鍵情報を用いて中間鍵を生成し、前記中間鍵を用いて、

コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、

前記中間鍵を暗号化して保持する保持手段とを備えた、著作権保護装置。

5．（補正後）前記鍵生成手段は、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理手段は、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持手段は、複数のメディアについて生成された前記中間鍵を、暗号化して保持することを特徴とする、請求項4に記載の著作権保護装置。

6．コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより、コンテンツに暗号処理を行うための鍵と、前記鍵を生成するための中間鍵とを生成する鍵生成手段と、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、

前記中間鍵および前記鍵生成用データの少なくとも一方を保持する保持手段とを備えた、著作権保護装置。

7．前記鍵生成手段は、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理手段は、各メディアごとに生成された前記

鍵を用いて、コンテンツに暗号処理を行い、

前記保持手段は、前記中間鍵および前記鍵生成用データを各メディアごとに保持することを特徴とする、請求項6に記載の著作権保護装置。

8．（補正後）コンテンツの暗号化または暗号復号を行う著作権保護方法であって、

メディアおよび前記メディアの記録再生装置に蓄積された鍵情報を用いて中間鍵を生成し、前記中間鍵を用いて、コンテンツに暗号処理を行うための鍵を生成する鍵生成ステップと、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、

前記中間鍵を鍵として認識できない形式で保持する保持ステップとを備えた、著作権保護方法。

9．（補正後）前記鍵生成ステップは、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理ステップは、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持ステップは、複数のメディアについて生成された前記中間鍵を、鍵として認識できない形式で保持することを特徴とする、請求項8に記載の著作権保護方法。

10．（補正後）コンテンツの暗号化または暗号復号を行う著作権保護方法であって、

メディアおよび前記メディアの記録再生装置に蓄積された鍵情報を用いて中間鍵を生成し、前記中間鍵を用いて、コンテンツに暗号処理を行うための鍵を生成する鍵生成ス

テップと

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、

前記中間鍵を暗号化して保持する保持ステップとを備えた、著作権保護方法。

１１．　コンテンツの暗号化または暗号復号を行う著作権保護方法であって、

行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより、コンテンツに暗号処理を行うための鍵と、前記鍵を生成するための中間鍵とを生成する鍵生成テップと、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、

前記中間鍵および前記鍵生成用データの少なくとも一方を保持する保持ステップとを備えた、著作権保護方法。

１２．　前記鍵生成ステップは、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理ステップは、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持ステップは、前記中間鍵および前記鍵生成用データを各メディアごとに保持することを特徴とする、請求項１１に記載の著作権保護方法。

１３．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段

図１

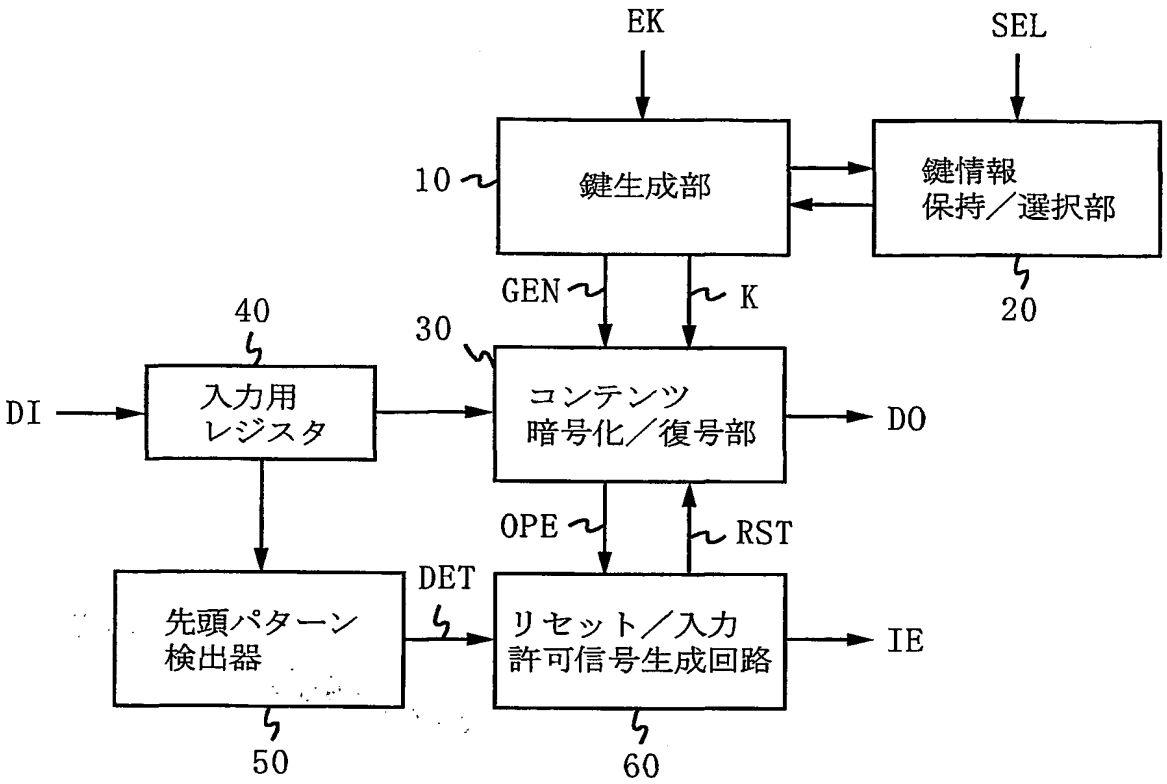

EK
SEL
10
鍵生成部
鍵情報
保持／選択部
20
GEN
K
40
30
DI
入力用
レジスタ
コンテンツ
暗号化／復号部
DO
OPE
RST
DET
先頭パターン
検出器
リセット／入力
許可信号生成回路
IE
50
60

図２

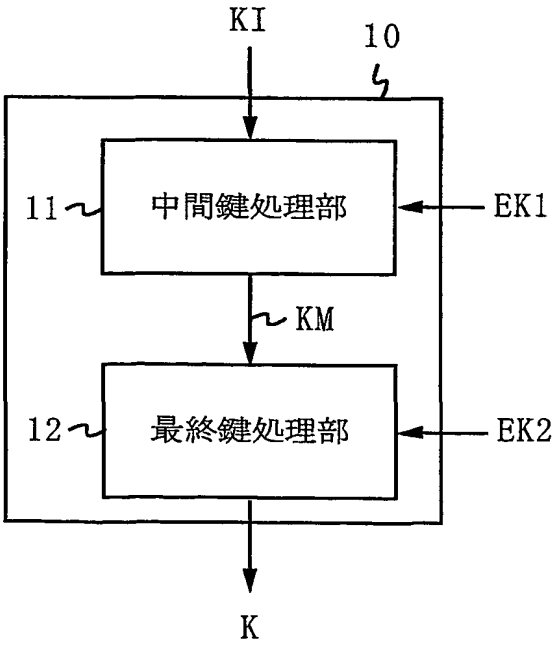

KI
10
11
中間鍵処理部
EK1
KM
12
最終鍵処理部
EK2
K

図３

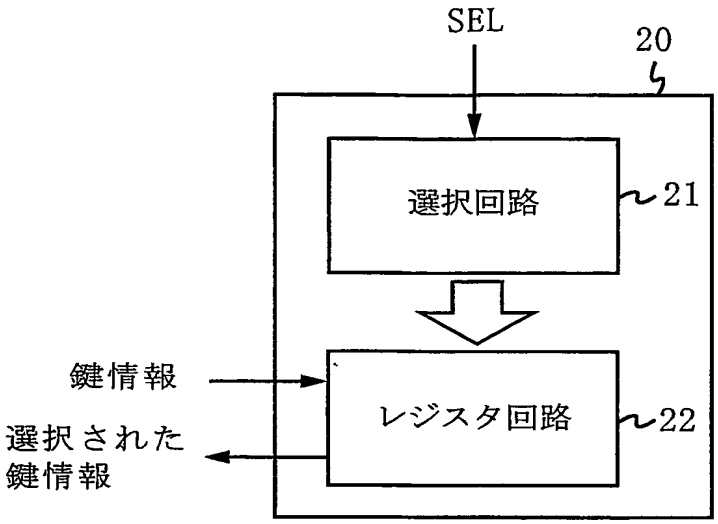

SEL
20
選択回路
21
鍵情報
選択された
鍵情報
レジスタ回路
22

図４

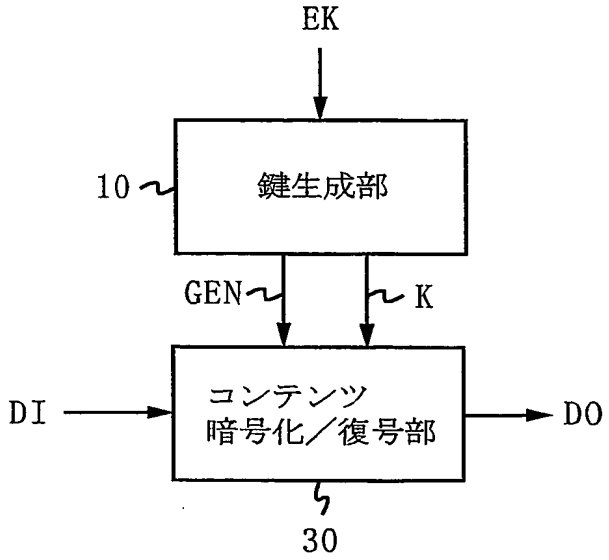

EK
10
鍵生成部
GEN
K
DI
コンテンツ
暗号化／復号部
DO
30

図５

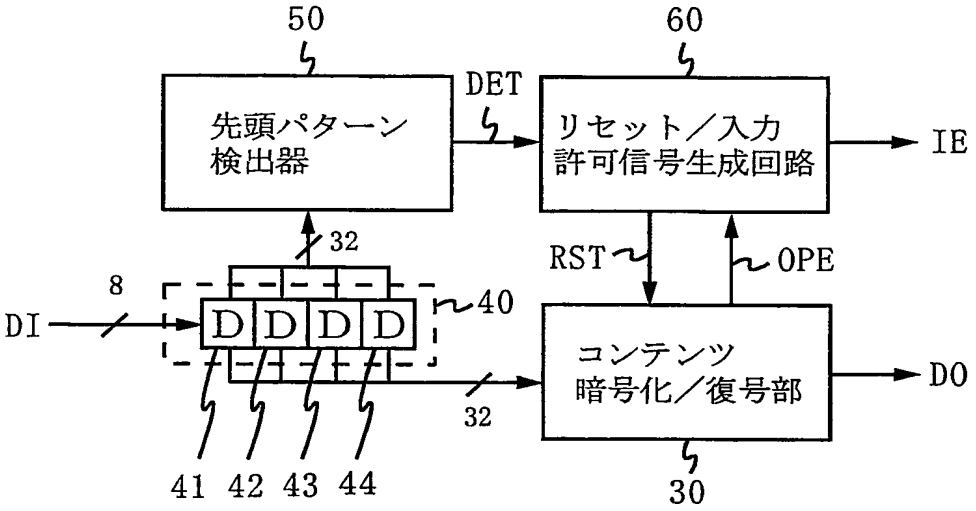

50
60
DET
先頭パターン
検出器
リセット／入力
許可信号生成回路
IE
32
RST
OPE
8
DI
D D D D
40
コンテンツ
暗号化／復号部
DO
32
41 42 43 44
30

図６

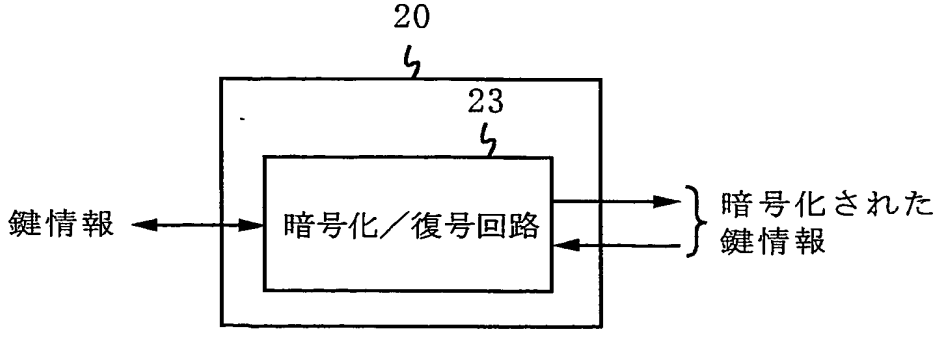

20
23
鍵情報
暗号化／復号回路
暗号化された
鍵情報

図７

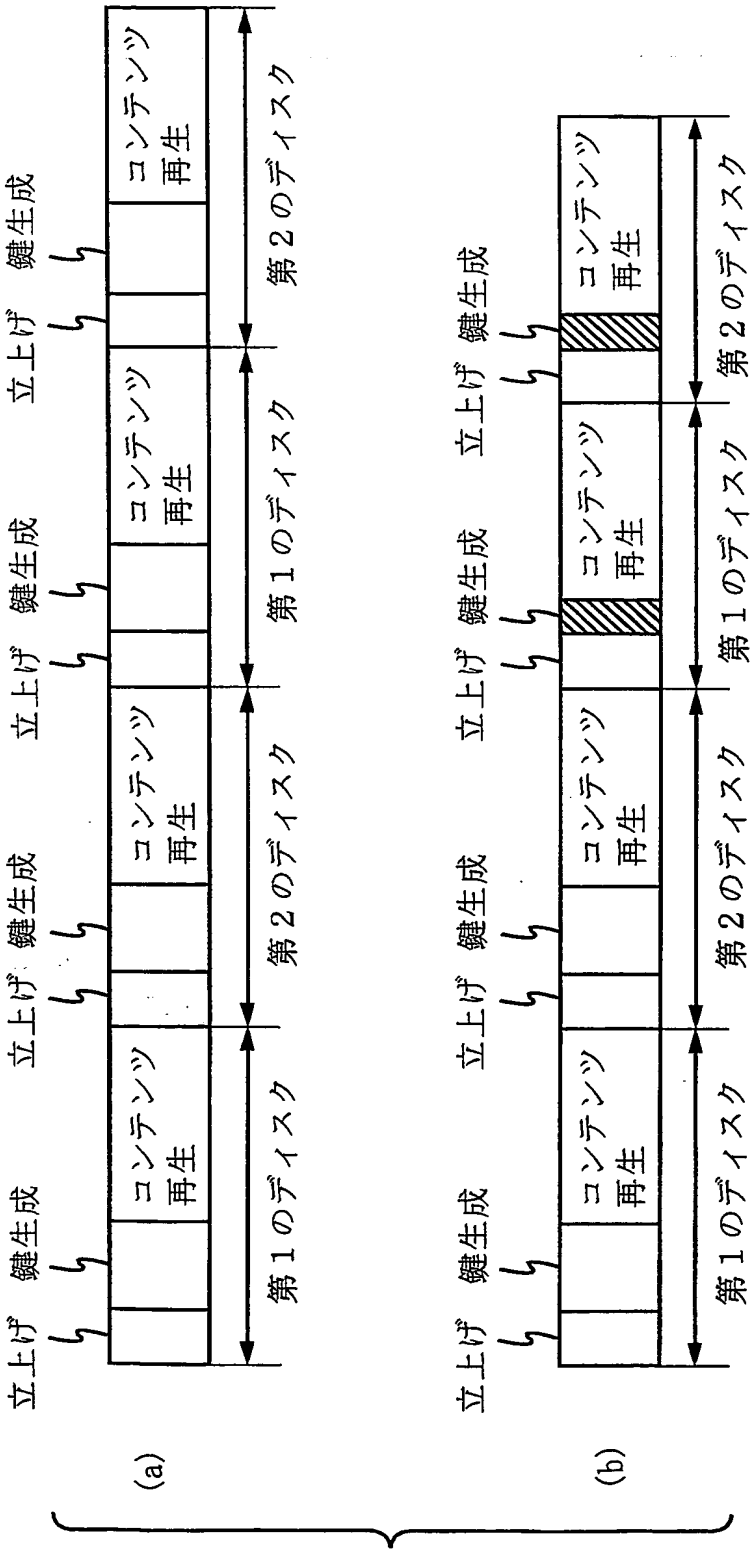


図８

バイト	ビット 7-0
0	記録タイプ：01(16進数)
1-3	記録長：ｎ
4-5	予約領域
6-7	バージョン
8	列
9-11	世代：000001(16進数)
12-19	行０に対する暗号化された鍵情報
20-27	行１に対する暗号化された鍵情報
28～n-1	行ｉに対する暗号化された鍵情報

図９

バイト	ビット 7-0	
0	記録タイプ：82(16進数)	記録データヘッダ
1-3	記録長：ｎ	
4-7	暗号化された検証データ：DEADBEEF(16進数)	
8	暗号化された列	
9-11	暗号化された世代：000001(16進数)	
12-19	行０に対する二重に暗号化された鍵情報	記録データ
20-27	行１に対する二重に暗号化された鍵情報	
28～n-1	行ｉに対する二重に暗号化された鍵情報	

図１０

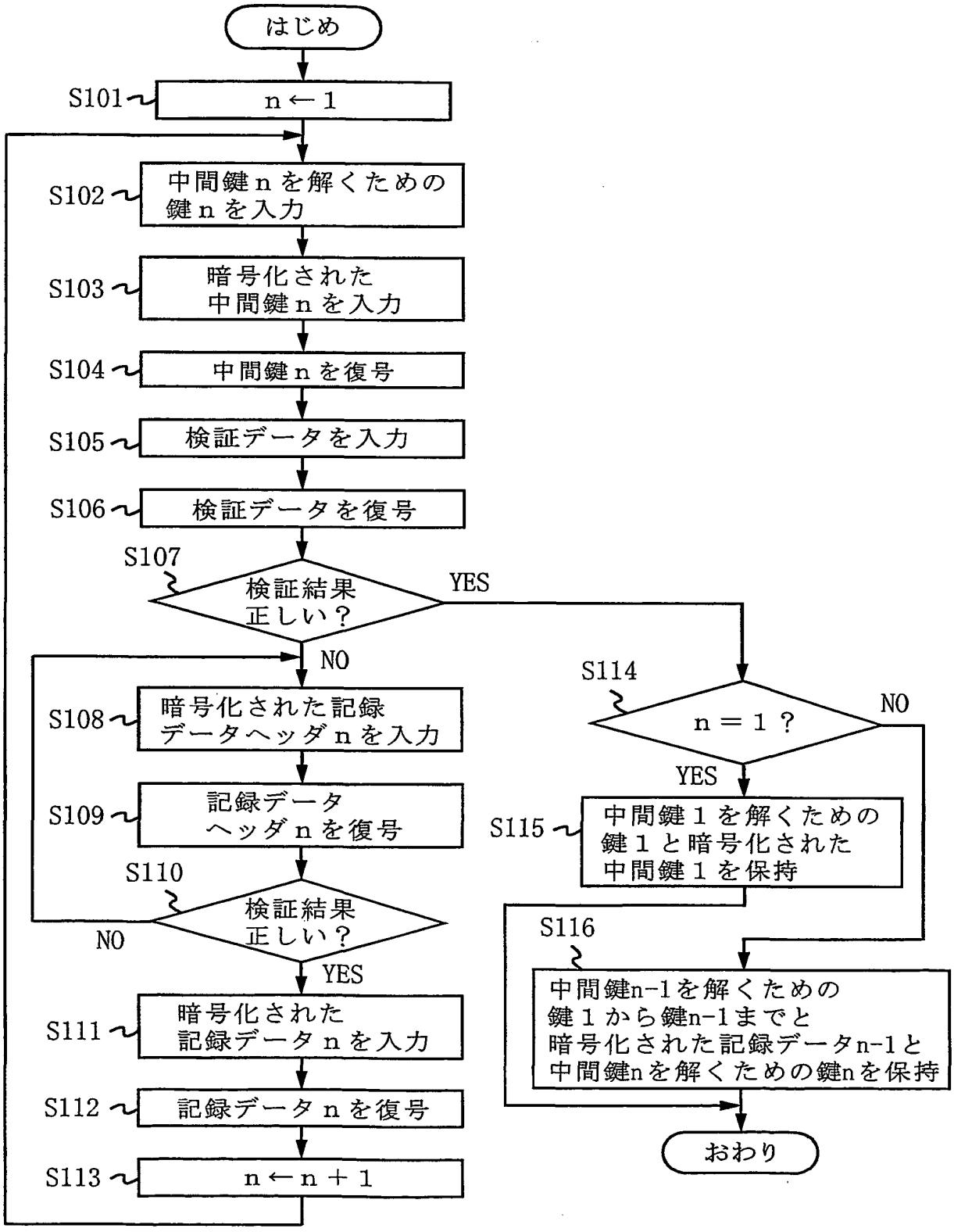

はじめ
S101
n←1
S102
中間鍵nを解くための鍵nを入力
S103
暗号化された中間鍵nを入力
S104
中間鍵nを復号
S105
検証データを入力
S106
検証データを復号
S107
検証結果正しい？
YES
NO
S108
暗号化された記録データヘッダnを入力
S109
記録データヘッダnを復号
S110
検証結果正しい？
NO
YES
S111
暗号化された記録データnを入力
S112
記録データnを復号
S113
n←n＋1
S114
n＝1？
NO
YES
S115
中間鍵1を解くための鍵1と暗号化された中間鍵1を保持
S116
中間鍵n-1を解くための鍵1から鍵n-1までと暗号化された記録データn-1と中間鍵nを解くための鍵nを保持
おわり

図１１

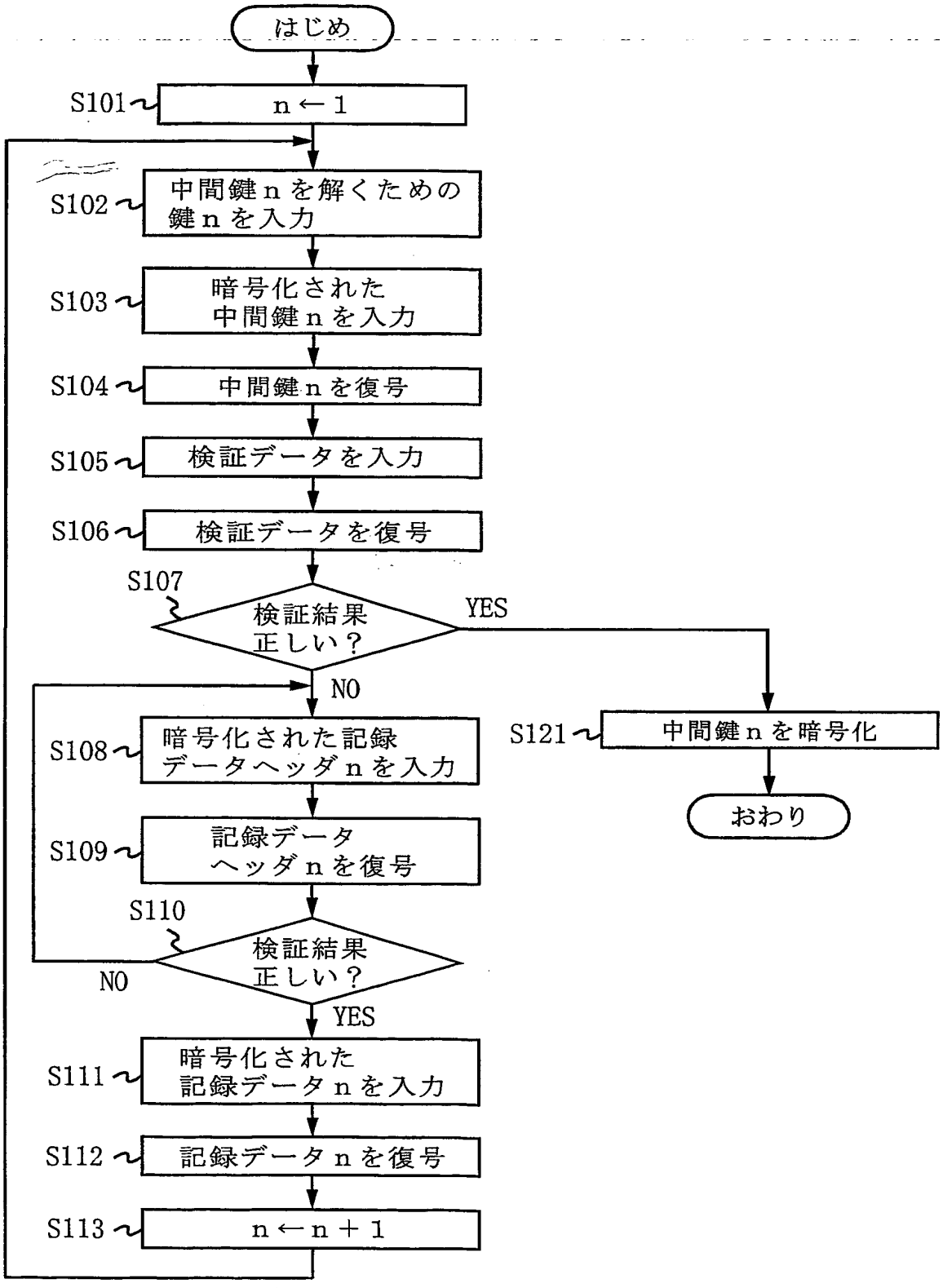

はじめ
S101
n←1
S102
中間鍵nを解くための鍵nを入力
S103
暗号化された中間鍵nを入力
S104
中間鍵nを復号
S105
検証データを入力
S106
検証データを復号
S107
検証結果正しい？
YES
NO
S108
暗号化された記録データヘッダnを入力
S109
記録データヘッダnを復号
S110
検証結果正しい？
NO
YES
S111
暗号化された記録データnを入力
S112
記録データnを復号
S113
n←n＋1
S121
中間鍵nを暗号化
おわり

図１２

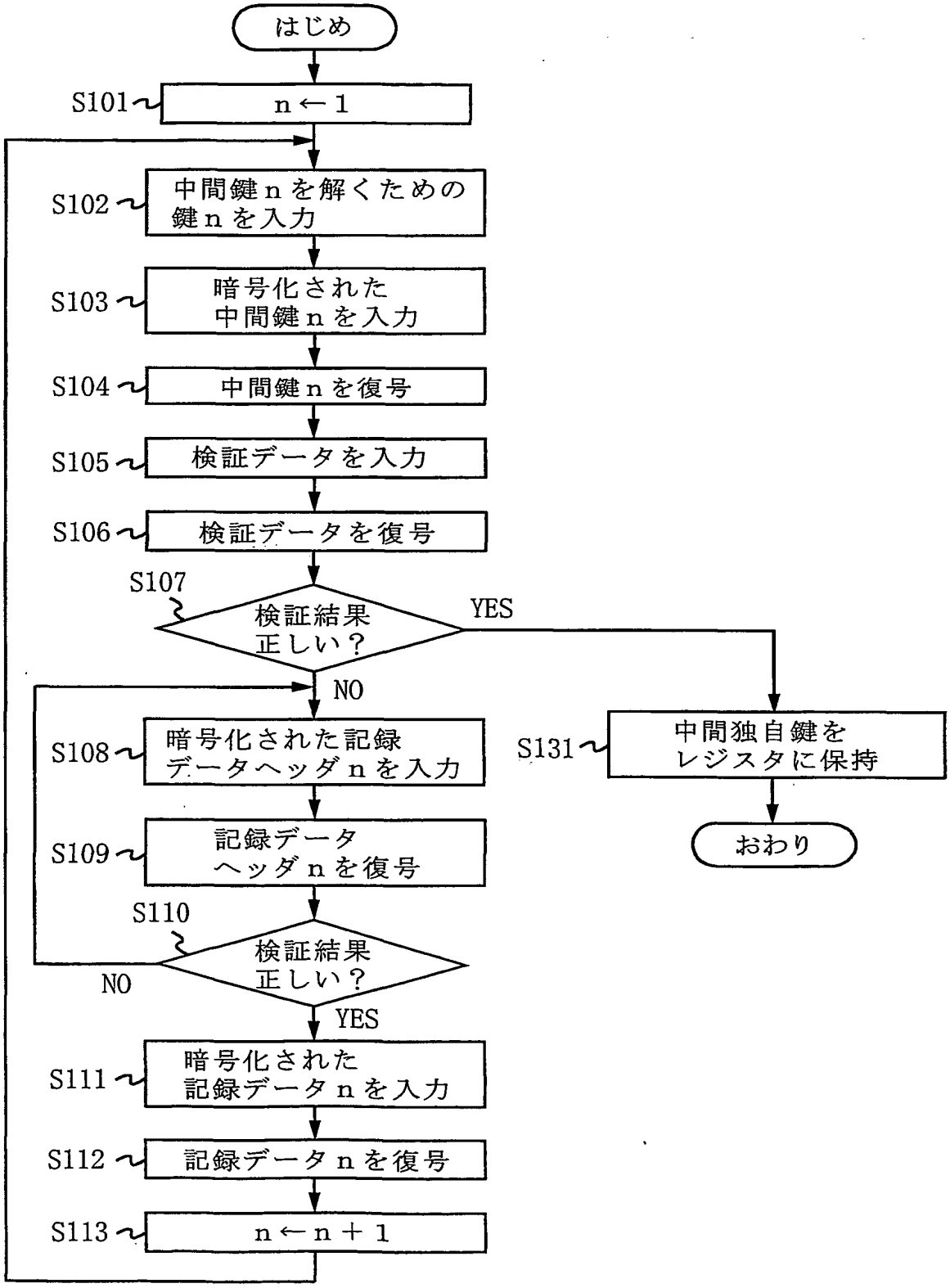

はじめ
S101
n←1
S102
中間鍵nを解くための鍵nを入力
S103
暗号化された中間鍵nを入力
S104
中間鍵nを復号
S105
検証データを入力
S106
検証データを復号
S107
検証結果正しい？
YES
NO
S131
中間独自鍵をレジスタに保持
おわり
S108
暗号化された記録データヘッダnを入力
S109
記録データヘッダnを復号
S110
検証結果正しい？
NO
YES
S111
暗号化された記録データnを入力
S112
記録データnを復号
S113
n←n＋1

図１３

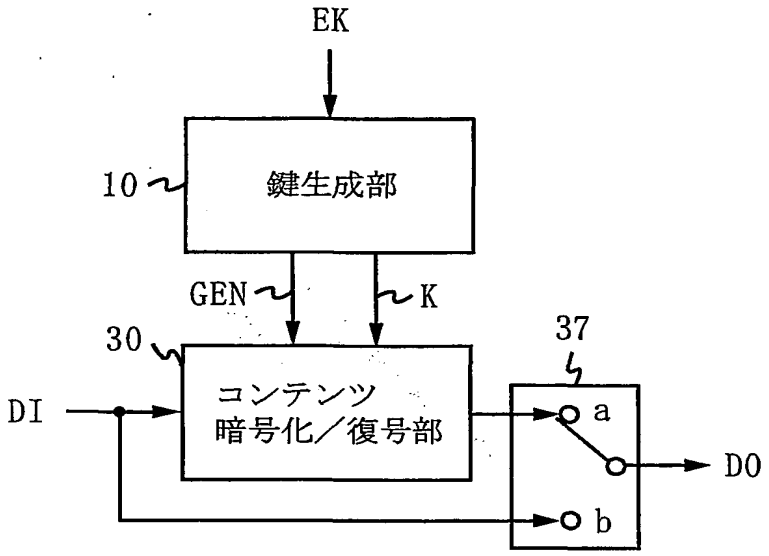


図１４

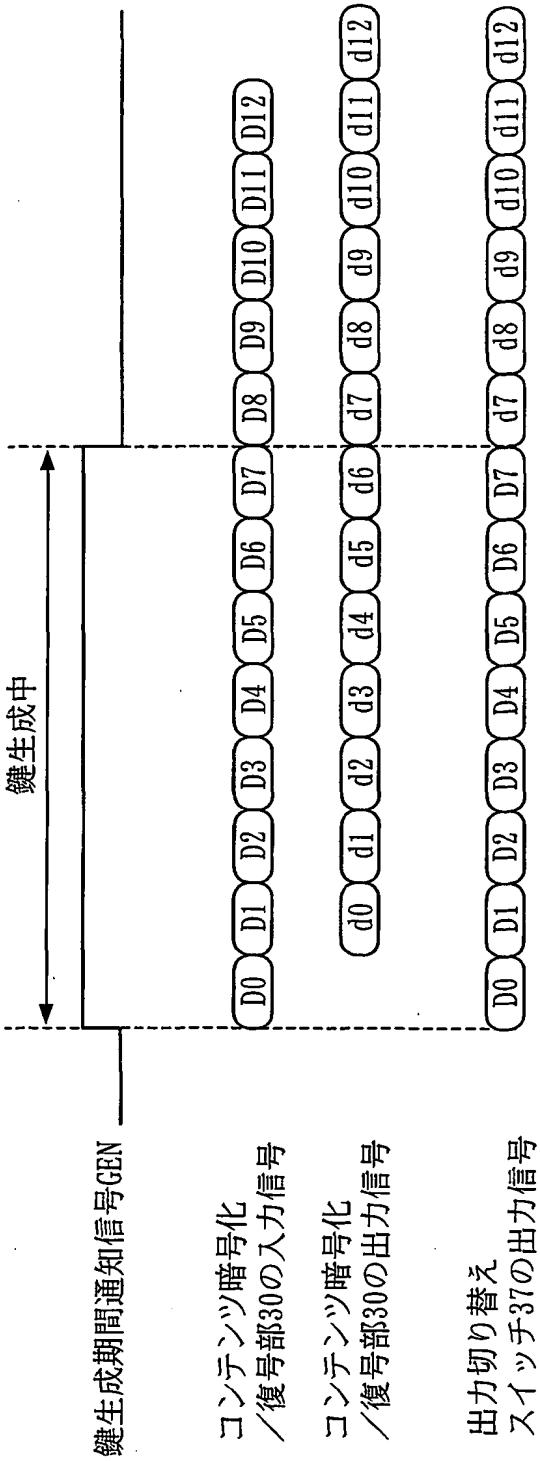

鍵生成中
鍵生成期間通知信号GEN
コンテンツ暗号化
／復号部30の入力信号
コンテンツ暗号化
／復号部30の出力信号
出力切り替え
スイッチ37の出力信号
D0 D1 D2 D3 D4 D5 D6 D7 D8 D9 D10 D11 D12
d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 d10 d11 d12
D0 D1 D2 D3 D4 D5 D6 D7 d7 d8 d9 d10 d11 d12

図１５

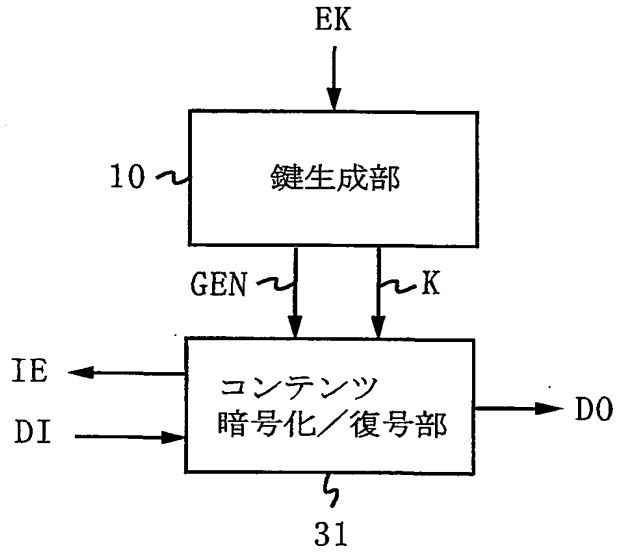
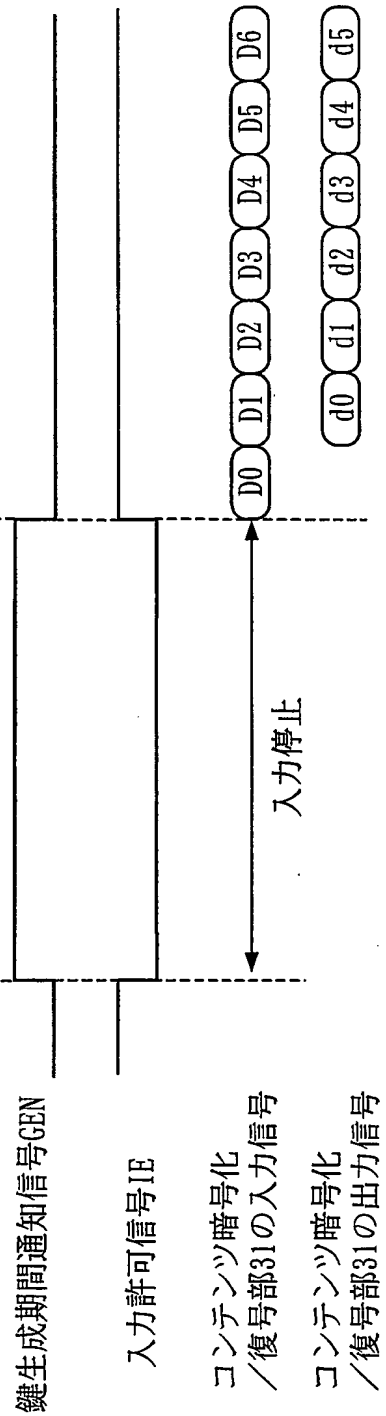


図１６


鍵生成中
入力停止
D0
D1
D2
D3
D4
D5
D6
d0
d1
d2
d3
d4
d5
鍵生成期間通知信号GEN
入力許可信号IE
コンテンツ暗号化
／復号部31の入力信号
コンテンツ暗号化
／復号部31の出力信号

THIS PAGE BLANK

図１７

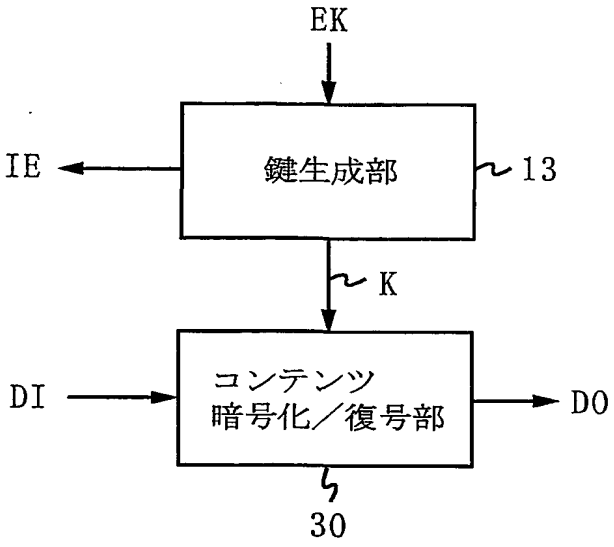

EK
鍵生成部
13
IE
K
DI
コンテンツ
暗号化／復号部
DO
30

図１８

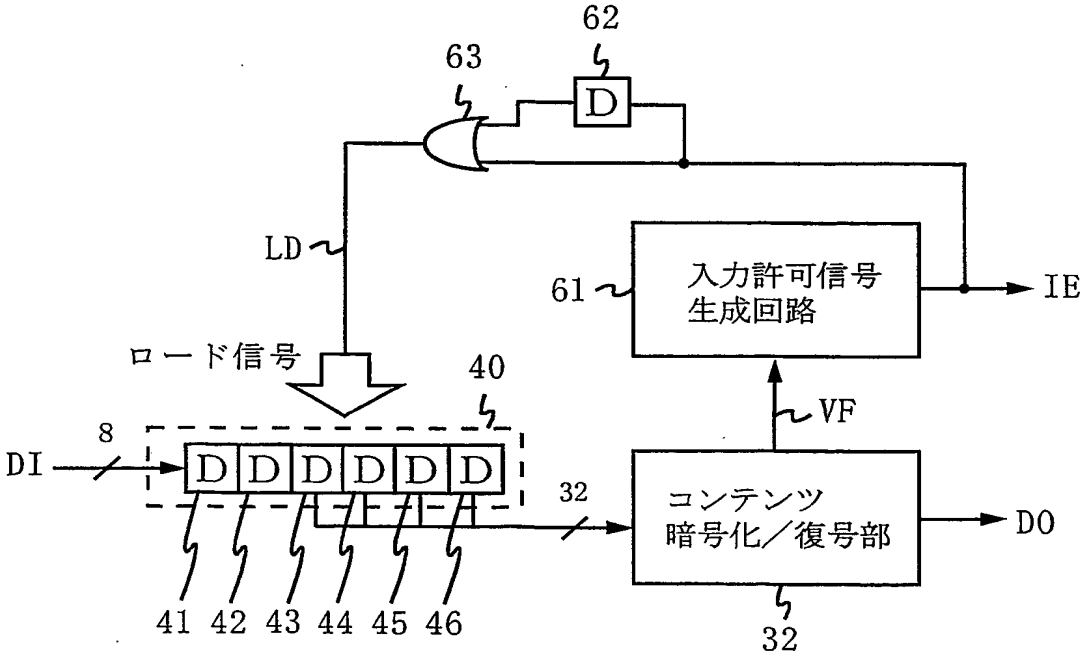

62
63
D
LD
61
入力許可信号
生成回路
IE
ロード信号
40
VF
8
DI
D D D D D D
32
コンテンツ
暗号化／復号部
DO
41 42 43 44 45 46
32

図１９

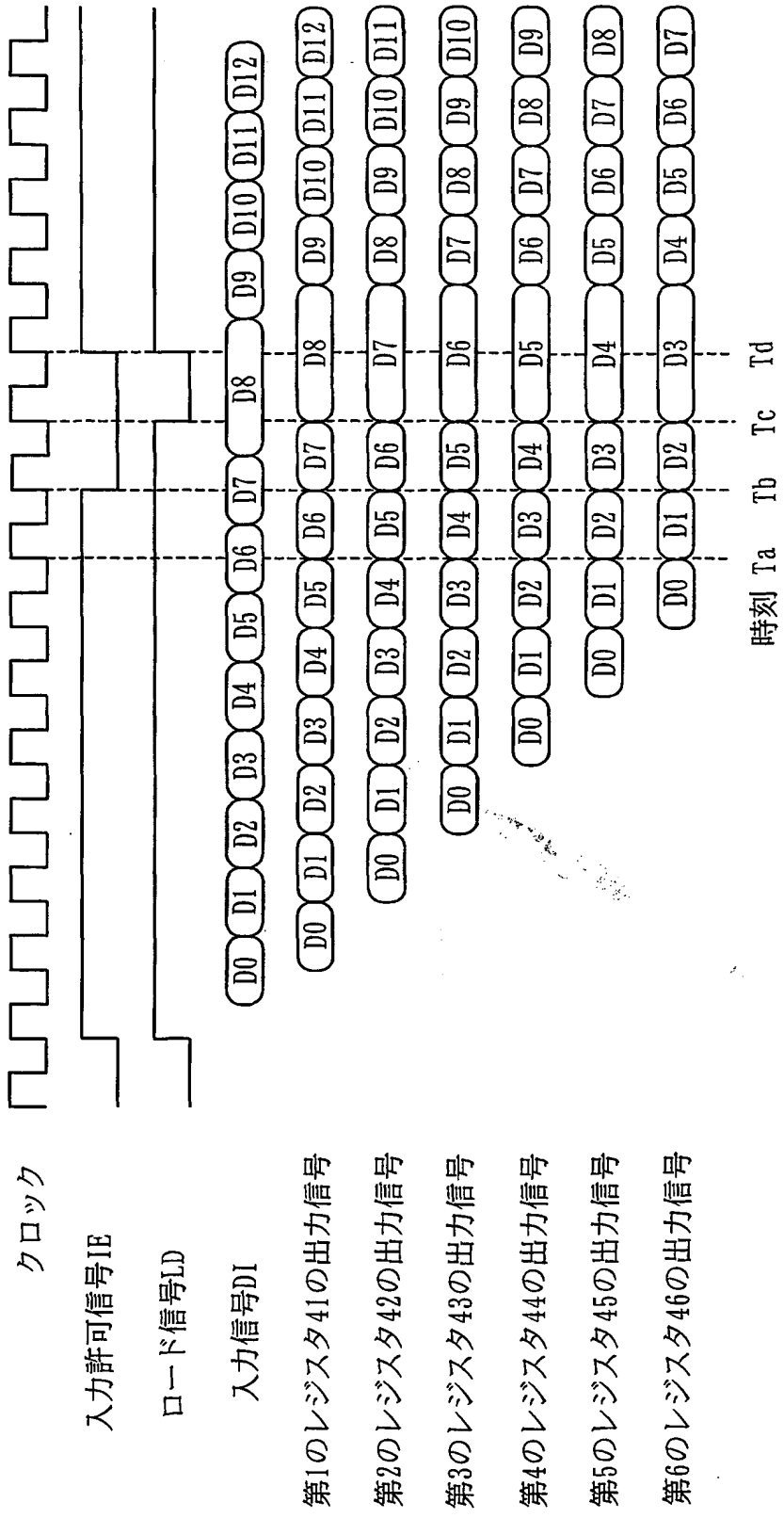

クロック
入力許可信号IE
ロード信号LD
入力信号DI
第1のレジスタ41の出力信号
第2のレジスタ42の出力信号
第3のレジスタ43の出力信号
第4のレジスタ44の出力信号
第5のレジスタ45の出力信号
第6のレジスタ46の出力信号
D0 D1 D2 D3 D4 D5 D6 D7 D8 D9 D10 D11 D12
時刻 Ta Tb Tc Td

図２０

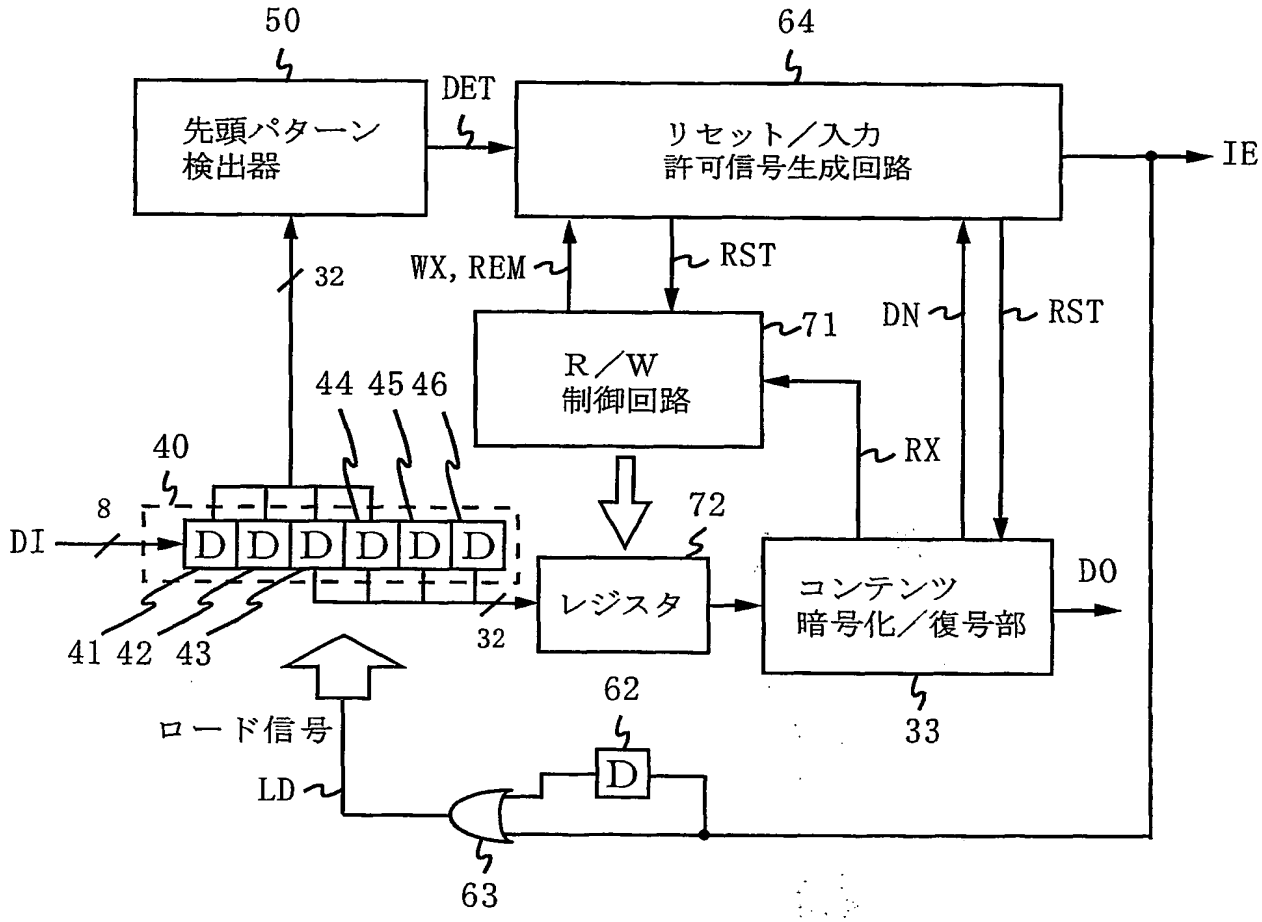

50
64
先頭パターン
検出器
DET
リセット／入力
許可信号生成回路
IE
32
WX, REM
RST
71
DN
RST
R／W
制御回路
44 45 46
40
RX
8
DI
D D D D D D
72
レジスタ
コンテンツ
暗号化／復号部
DO
41 42 43
32
62
33
ロード信号
D
LD
63

図２１

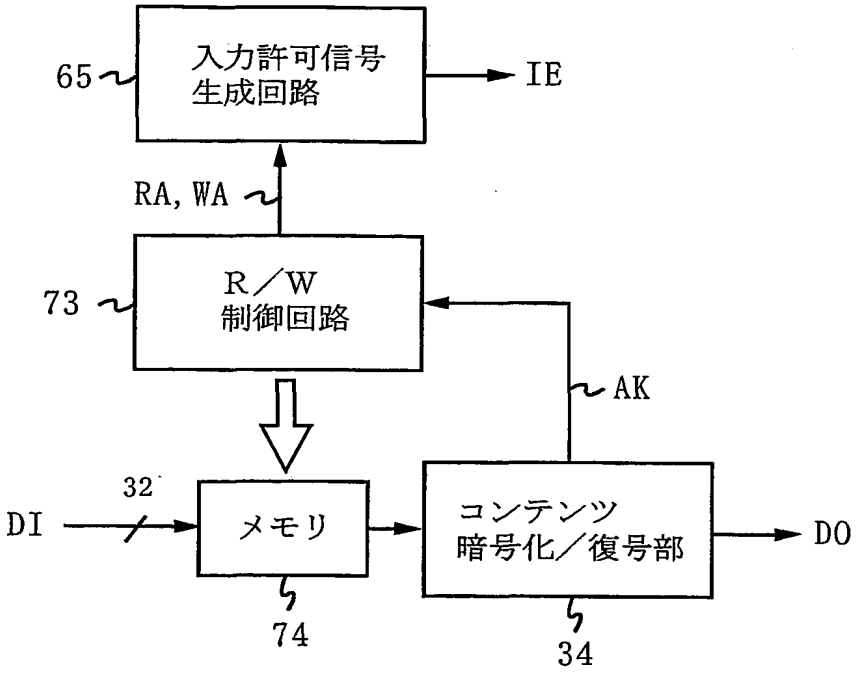
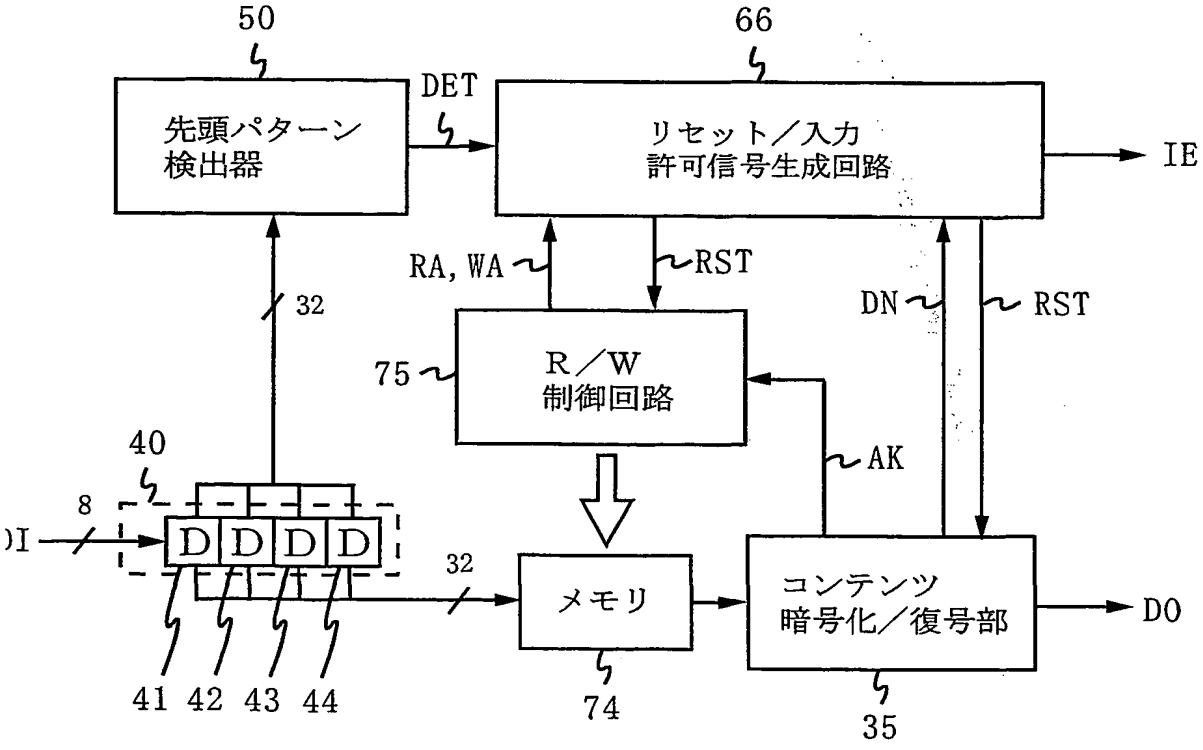

65
入力許可信号
生成回路
IE
RA, WA
73
R／W
制御回路
AK
32
DI
メモリ
コンテンツ
暗号化／復号部
DO
74
34

図２２


50
66
先頭パターン
検出器
DET
リセット／入力
許可信号生成回路
IE
RA, WA
RST
32
DN
RST
75
R／W
制御回路
AK
40
8
DI
D D D D
32
メモリ
コンテンツ
暗号化／復号部
DO
41 42 43 44
74
35

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05484

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/00, G11B20/10, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/00, G11B20/10, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, JICST FILE on Science and Technology content, key, encryption, DVD

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 00/22539 A1 (Sony Corporation), 20 April, 2000 (20.04.00), page 100, lines 8 to 15; page 101, lines 1 to 4; page 122, line 12 to page 123, line 3 & JP 2000-123084 A & JP 2000-124890 A & JP 2000-138673 A & JP 2000-188595 A & AU 9961231 A & EP 1039392 A1 & CN 1289421 A	1,4,8,10 2,3,5,9
Y	JP 10-293724 A (Toshiba Corporation), 04 November, 1998 (04.11.98), Par. Nos. [0039] to [0076] (Family: none)	2,3,5,9
A	JP 11-39794 A (Matsushita Electric Ind. Co., Ltd.), 12 February, 1999 (12.02.99), Full text (Family: none)	1-5,8-10
A	JP 2000-122539 A (Matsushita Electric Ind. Co., Ltd.), 28 April, 2000 (28.04.00), Par. Nos. [0018], [0044], [0045] (Family: none)	1-5,8-10

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 September, 2001 (11.09.01)	25 September, 2001 (25.09.01)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05484

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The examiner has judged that the inventions of claims of the international application are divided into eight groups. However, according to the decision on the protest against the additional fee, the inventions are divided into seven groups.

1. The inventions of claims 1-5, 8-10
2. The inventions of claims 6, 7, 11, 12
3. The inventions of claims 13, 14
4. The inventions of claims 15, 16
5. The invention of claim 17
6. The invention of claim 18
7. The invention of claim 19

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☒ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

Claims 1 to 5, 8 to 10

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☒ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/05484

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Supervision: Shin ICHIMATSU, "Data Hogo to Angou-ka no Kenkyuu; Computer Network no Anzensei", Nippon Keizai Shinbunsha, 29 July, 1983 (29.07.83), pages 201 to 206 (especially, page 204, 3 Data Angou Kagi no Touroku)	1-5,8-10

国際調査報

国際出願番号 PCT／JP01／05484

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9／00, G11B20／10, G06F15／00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9／00, G11B20／10, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI, JICST科学技術文献データベース content, key, encryption, DVD

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	WO 00/22539 A1 (ソニー株式会社) 20. 4月.2000(20.04.00), 第100頁第8-15行, 第101頁第1-4行, 第122頁第12行－第123頁第3行 & JP 2000-123084 A & JP 2000-124890 A & JP 2000-138673 A & JP 2000-188595 A & AU 9961231 A & EP 1039392 A1 & CN 1289421 A	1, 4, 8, 10 2, 3, 5, 9
Y	JP 10-293724 A (株式会社東芝) 4.11月.1998(04.11.98), 第39-76段落 (ファミリなし)	2, 3, 5, 9
A	JP 11-39794 A (松下電器産業株式会社) 12. 2月.1999(12.02.99), 全頁を参照 (ファミリなし)	1-5, 8-10

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 11. 09. 01	国際調査報告の発送日 25.09.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里 裕正 5M 9364 電話番号 03－3581－1101 内線 3597

国[redacted]査報告

国際[redacted]番号　PCT／JP01／05484

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

審査官は、この出願の発明は８群に区分されると認定したが、追加手数料異議の申立ての決定の結果、以下の７群となった。

1．請求の範囲 1-5, 8-10
2．請求の範囲 6, 7, 11, 12
3．請求の範囲13, 14
4．請求の範囲15, 16
5．請求の範囲17
6．請求の範囲18
7．請求の範囲19

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☒ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

請求の範囲 1-5, 8-10

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☒ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2000-122539 A （松下電器産業株式会社） 28. 4月. 2000(28. 04. 00)，第18, 44, 45段落（ファミリなし）	1-5, 8-10
A	一松信 監修，データ保護と暗号化の研究 コンピュータ・ネットワークの安全性，日本経済新聞社，29. 7月. 1983(29. 07. 83)， p. 201-206 （特にp. 204 3データ暗号鍵の登録 を参照）	1-5, 8-10

Replaced by Article 19

CLAIMS

1. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content,

cryptographic processing means for applying cryptographic processing to the content by using the key, and

retention means for retaining, in a form which is not recognizable as a key, at least one of an intermediate key for generating the key and the key.

2. The copyright protective device according to claim 1, wherein,

the key generation means generates said key with respect to each of a plurality of media, and

the cryptographic processing means applies cryptographic processing to the content by using the key generated for each medium.

3. The copyright protective device according to claim 1, wherein the retention means retains the intermediate key and the key in a storage circuit within integrated circuitry.

4. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content,

cryptographic processing means for applying cryptographic processing to the content by using the key, and

retention means for retaining at least one of an intermediate key for generating the key and the key in an encrypted manner.

5. The copyright protective device according to claim 4, wherein,

the key generation means generates said key with respect to each of a plurality of media, and

the cryptographic processing means applies cryptographic processing to the content by using the key generated for each medium.

6. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content and an intermediate key for generating the key, by sequentially extracting necessary data from key generation data which is formed in a matrix and applying computation processing thereto,

cryptographic processing means for applying cryptographic processing to the content by using the key, and

retention means for retaining at least one of the intermediate key and the key generation data.

7. The copyright protective device according to claim 6, wherein,

the key generation means generates said key with respect to each of a plurality of media,

the cryptographic processing means applies cryptographic processing to the content by using the key generated for each medium, and

the retention means retains the intermediate key and the key generation data with respect to each medium.

8. A copyright protective method for encrypting or decrypting a content, comprising:

a key generation step of generating a key with which to apply cryptographic processing to the content,

an cryptographic processing step of applying cryptographic processing to the content by using the key, and

a retention step of retaining, in a form which is not recognizable as a key, at least one of an intermediate key for generating the key and the key.

9. The copyright protective method according to claim 8, wherein,

the key generation step generates said key with respect to each of a plurality of media, and

the cryptographic processing step applies cryptographic processing to the content by using the key generated for each medium.

10. A copyright protective method for encrypting or decrypting a content, comprising:

a key generation step of generating a key with which to apply cryptographic processing to the content,

an cryptographic processing step of applying cryptographic processing to the content by using the key, and

a retention step of retaining at least one of an intermediate key for generating the key and the key in an encrypted manner.

11. A copyright protective method for encrypting or decrypting a content, comprising:

a key generation step of generating a key with which to apply cryptographic processing to the content and an intermediate key for generating the key, by sequentially extracting necessary data from key generation data which is formed in a matrix and applying computation processing thereto,

an cryptographic processing step of applying cryptographic processing to the content by using the key, and

a retention step of retaining at least one of the intermediate key and the key generation data.

12. The copyright protective method according to claim 11, wherein,

the key generation step generates said key with respect to each of a plurality of media,

the cryptographic processing step applies cryptographic processing to the content by using the key generated for each medium, and

the retention step retains the intermediate key and the key generation data with respect to each medium.

13. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not, and

cryptographic processing means, to which a content containing identification information indicating whether or not to perform cryptographic processing is inputted, for applying cryptographic processing to the content in accordance with the identification information by using the key, and for outputting a result of the cryptographic processing,

wherein the cryptographic processing means restrains the result of the cryptographic processing from being outputted when the notification signal indicates that key generation is being performed.

14. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not,

cryptographic processing means, to which a content

containing an identification signal indicating whether or not to perform cryptographic processing is inputted, for applying cryptographic processing to the content in accordance with the identification signal by using the key, and for outputting a result of the cryptographic processing, and

selection means for selecting a content which is inputted to the cryptographic processing means when the notification signal indicates that key generation is being performed, and otherwise selecting the result of the cryptographic processing outputted from the cryptographic processing means.

15. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not, and

cryptographic processing means, to which a content containing an identification signal indicating whether or not to perform cryptographic processing is inputted, for applying cryptographic processing to the content in accordance with the identification signal by using the key, and for outputting a result of the cryptographic processing,

wherein, when the notification signal indicates that key generation is being performed, the cryptographic processing means switches an input enable signal for controlling inputting of

contents to an input disabled state.

16. A copyright protective device for encrypting or decrypting a content, comprising:

key generation means for generating a key with which to apply cryptographic processing to the content, and

cryptographic processing means, to which a content containing an identification signal indicating whether or not to perform cryptographic processing is inputted, for applying cryptographic processing to the content in accordance with the identification signal by using the key, and for outputting a result of the cryptographic processing,

wherein, when key generation is being performed, the key generation means switches an input enable signal for controlling inputting of contents to an input disabled state.

17. A signal processing device for processing an input signal containing per plurality of symbols a heading pattern which represents a heading of a processing unit, comprising:

a register for retaining the input signal which is sequentially inputted,

heading pattern detection means for detecting the heading pattern being contained in the input signal retained in the register,

signal processing means for applying predetermined signal processing to the input signal which is supplied via the register, and notifying whether the input signal is being processed or not,

and

control signal generation means which outputs a reset signal to the signal processing means if the signal processing means is not performing processing when the heading pattern is detected by the heading pattern detection means, and if the signal processing means is performing processing when the heading pattern is detected by the heading pattern detection means, switches an input enable signal for controlling input to an input disabled state and transitions to a reset-waiting state, and outputs a reset signal to the signal processing means when the processing by the signal processing means is completed in the reset-waiting state.

18. A signal processing device for processing an input signal which is inputted symbol by symbol in accordance with an input enable signal,

signal processing means to which not more than *c* symbols of said input signal is inputted after the input enable signal changes to an input disabled state, wherein the signal processing means processes *b* symbols of said signal at one time and notifies an overflow state of internal processing,

input enable signal generation means for switching the input enable signal to an input disabled state when the processing by the signal processing means enters an overflow state, and

a register which retains *a* symbols of said input signal, outputs *b* symbols to the signal processing means when the input

enable signal is in an input enabled state, wherein a, b, and c are of the relationship $a \geqq (b+c)$, and employs as a load signal a logical OR signal between the input enable signal and a signal obtained by delaying the signal by one clock cycle.

19. A signal processing device for processing an input signal which is inputted symbol by symbol in accordance with an input enable signal,

signal processing means to which not more than c symbols of said input signal is inputted after the input enable signal changes to an input disabled state, wherein the signal processing means applies predetermined processing to the input signal and notifies whether the input signal is acceptable or not,

a memory for storing the input signal and outputting the stored input signal to the signal processing means,

memory control means which, if the input signal is acceptable to the signal processing means, controls the memory so that the data is read therefrom, and outputs a write address and a read address while performing write control so as not to overwrite data on any unread data, and

input enable signal generation means for switching the input enable signal to an input disabled state when a write margin which is calculated based on the write address and the read address outputted from the memory control means reaches at least c symbols.

請求の範囲

1．　（補正後）コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

メディアおよび前記メディアの記録再生装置に蓄積された鍵情報を用いて中間鍵を生成し、前記中間鍵を用いて、コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、

前記中間鍵を鍵として認識できない形式で保持する保持手段とを備えた、著作権保護装置。

2．　（補正後）前記鍵生成手段は、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理手段は、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持手段は、複数のメディアについて生成された前記中間鍵を、鍵として認識できない形式で保持することを特徴とする、請求項1に記載の著作権保護装置。

3．　前記保持手段は、前記中間鍵および前記鍵を集積回路内の記憶回路に保持することを特徴とする、請求項1に記載の著作権保護装置。

4．　（補正後）コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

メディアおよび前記メディアの記録再生装置に蓄積された鍵情報を用いて中間鍵を生成し、前記中間鍵を用いて、

ATTACHMENT C

コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、

前記中間鍵を暗号化して保持する保持手段とを備えた、著作権保護装置。

5．　（補正後）前記鍵生成手段は、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理手段は、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持手段は、複数のメディアについて生成された前記中間鍵を、暗号化して保持することを特徴とする、請求項４に記載の著作権保護装置。

6．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより、コンテンツに暗号処理を行うための鍵と、前記鍵を生成するための中間鍵とを生成する鍵生成手段と、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理手段と、

前記中間鍵および前記鍵生成用データの少なくとも一方を保持する保持手段とを備えた、著作権保護装置。

7．　前記鍵生成手段は、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理手段は、各メディアごとに生成された前記

鍵を用いて、コンテンツに暗号処理を行い、

前記保持手段は、前記中間鍵および前記鍵生成用データを各メディアごとに保持することを特徴とする、請求項6に記載の著作権保護装置。

8．　（補正後）コンテンツの暗号化または暗号復号を行う著作権保護方法であって、

メディアおよび前記メディアの記録再生装置に蓄積された鍵情報を用いて中間鍵を生成し、前記中間鍵を用いて、コンテンツに暗号処理を行うための鍵を生成する鍵生成ステップと、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、

前記中間鍵を鍵として認識できない形式で保持する保持ステップとを備えた、著作権保護方法。

9．　（補正後）前記鍵生成ステップは、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理ステップは、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持ステップは、複数のメディアについて生成された前記中間鍵を、鍵として認識できない形式で保持することを特徴とする、請求項8に記載の著作権保護方法。

10．　（補正後）コンテンツの暗号化または暗号復号を行う著作権保護方法であって、

メディアおよび前記メディアの記録再生装置に蓄積された鍵情報を用いて中間鍵を生成し、前記中間鍵を用いて、コンテンツに暗号処理を行うための鍵を生成する鍵生成ス

テップと

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、

前記中間鍵を暗号化して保持する保持ステップとを備えた、著作権保護方法。

１１．　コンテンツの暗号化または暗号復号を行う著作権保護方法であって、

行列状に形成された鍵生成用データから順次必要なデータを抽出して演算処理を行うことにより、コンテンツに暗号処理を行うための鍵と、前記鍵を生成するための中間鍵とを生成する鍵生成テップと、

前記鍵を用いて、コンテンツに暗号処理を行う暗号処理ステップと、

前記中間鍵および前記鍵生成用データの少なくとも一方を保持する保持ステップとを備えた、著作権保護方法。

１２．　前記鍵生成ステップは、複数のメディアのそれぞれについて前記鍵を生成し、

前記暗号処理ステップは、各メディアごとに生成された前記鍵を用いて、コンテンツに暗号処理を行い、

前記保持ステップは、前記中間鍵および前記鍵生成用データを各メディアごとに保持することを特徴とする、請求項１１に記載の著作権保護方法。

１３．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段

と、

暗号処理を行うか否かを示す識別情報を含んだコンテンツが入力され、前記識別情報に従って前記鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段とを備え、

前記暗号処理手段は、前記通知信号が鍵生成中を示す場合は、前記暗号処理結果の出力を抑制することを特徴とする、著作権保護装置。

１４．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段と、

暗号処理を行うか否かを示す識別信号を含んだコンテンツが入力され、前記識別信号に従って前記鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段と、

前記通知信号が鍵生成中を示す場合は、前記暗号処理手段に入力されたコンテンツを選択し、それ以外の場合は、前記暗号処理手段から出力された暗号処理結果を選択して出力する選択手段とを備えた、著作権保護装置。

１５．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成するとともに、鍵生成中か否かを示す通知信号を出力する鍵生成手段と、

暗号処理を行うか否かを示す識別信号を含んだコンテンツが入力され、前記識別信号に従って前記鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段とを備え、

前記暗号処理手段は、前記通知信号が鍵生成中を示す場合は、コンテンツの入力を制御する入力許可信号を入力禁止状態に切り替えることを特徴とする、著作権保護装置。

１６．　コンテンツの暗号化または暗号復号を行う著作権保護装置であって、

コンテンツに暗号処理を行うための鍵を生成する鍵生成手段と、

暗号処理を行うか否かを示す識別信号を含んだコンテンツが入力され、前記識別信号に従って前記鍵を用いてコンテンツに暗号処理を行い、暗号処理結果を出力する暗号処理手段とを備え、

前記鍵生成手段は、鍵生成中は、コンテンツの入力を制御する入力許可信号を入力禁止状態に切り替えることを特徴とする、著作権保護装置。

１７．　複数のシンボルごとに処理単位の先頭を示す先頭パターンを含んだ入力信号を処理する信号処理装置であって、

順次入力された前記入力信号を保持するレジスタと、

前記レジスタに保持された入力信号に、前記先頭パターンが含まれていることを検出する先頭パターン検出手段と、

前記レジスタを経由して供給された前記入力信号に所定

の信号処理を行うとともに、前記入力信号を処理中か否かを通知する信号処理手段と、

前記先頭パターン検出手段が前記先頭パターンを検出したときに前記信号処理手段が処理中でない場合には、リセット信号を前記信号処理手段に出力し、前記先頭パターン検出手段が前記先頭パターンを検出したときに前記信号処理手段が処理中である場合には、入力を制御する入力許可信号を入力禁止状態に切り替えるとともにリセット待機状態に遷移し、リセット待機状態で前記信号処理手段における処理が完了したときに、リセット信号を前記信号処理手段に出力する制御信号生成手段とを備えた、信号処理装置。

１８．　入力許可信号に従ってシンボルごとに入力される入力信号を処理する信号処理装置であって、

前記入力許可信号が入力禁止状態に変化した後に高々ｃシンボル分の前記入力信号が入力され、前記入力信号を一度にｂシンボル分処理するとともに、内部処理のオーバーフロー状態を通知する信号処理手段と、

前記信号処理手段における処理がオーバーフロー状態となったときに、前記入力許可信号を入力禁止状態に切り替える入力許可信号生成手段と、

ａシンボル分の前記入力信号を保持し、前記入力許可信号が入力許可状態であるときにはｂシンボルを前記信号処理手段に出力し、前記ａと前記ｂと前記ｃとにはａ≧（ｂ＋ｃ）なる関係が成立し、前記入力許可信号と当該信号を１クロックサイクル遅延させた信号との論理和信号をロー

ド信号として用いるレジスタとを備えた、信号処理装置。

１９．　入力許可信号に従ってシンボルごとに入力される入力信号を処理する信号処理装置であって、

前記入力許可信号が入力禁止状態に変化した後に高々ｃシンボル分の前記入力信号が入力され、前記入力信号に所定の処理を行うとともに、前記入力信号を受け入れ可能か否かを通知する信号処理手段と、

前記入力信号を記憶し、記憶した前記入力信号を前記信号処理手段に対して出力するメモリと、

前記信号処理手段が前記入力信号を受け入れ可能である場合には、データが読み出されるように前記メモリを制御し、未だ読み出されていないデータには上書きしないように書き込み制御を行いながら、書き込みアドレスと読み出しアドレスとを出力するメモリ制御手段と、

前記メモリ制御手段から出力された書き込みアドレスと読み出しアドレスとに基づき算出した書き込み余裕量が少なくともｃシンボルになったときに、前記入力許可信号を入力禁止状態に切り替える入力許可信号生成手段とを備えた、信号処理装置。

US

10/069795

特　許　協　力　条　約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人 の書類記号　ＰＣＴ０１－０５２	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０１／０５４８４	国際出願日 （日.月.年）　２７．０６．０１	優先日 （日.月.年）　２９．０６．００
出願人（氏名又は名称） 松下電器産業株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　4　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☒ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☐ 出願人が提出したものを承認する。
☒ 次に示すように国際調査機関が作成した。

著作権保護装置及び方法

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　1　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報告

国際出願番号　T／JP01／05484

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

審査官は、この出願の発明は８群に区分されると認定したが、追加手数料異議の申立ての決定の結果、以下の７群となった。

1．請求の範囲 1-5, 8-10
2．請求の範囲 6, 7, 11, 12
3．請求の範囲13, 14
4．請求の範囲15, 16
5．請求の範囲17
6．請求の範囲18
7．請求の範囲19

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☒ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

請求の範囲 1-5, 8-10

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☒ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

国際調査報告

国際出願番号 [redacted]T／JP01／05484

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl' H04L9／00, G11B20／10, G06F15／00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl' H04L9／00, G11B20／10, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922－1996年
日本国公開実用新案公報 1971－2001年
日本国登録実用新案公報 1994－2001年
日本国実用新案登録公報 1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI, JICST科学技術文献データベース content, key, encryption, DVD

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	WO 00/22539 A1 (ソニー株式会社) 20. 4月.2000(20.04.00), 第100頁第8-15行, 第101頁第1-4行, 第122頁第12行－第123頁第3行 & JP 2000-123084 A & JP 2000-124890 A & JP 2000-138673 A & JP 2000-188595 A & AU 9961231 A & EP 1039392 A1 & CN 1289421 A	1, 4, 8, 10 2, 3, 5, 9
Y	JP 10-293724 A (株式会社東芝) 4.11月.1998(04.11.98), 第39-76段落 (ファミリなし)	2, 3, 5, 9
A	JP 11-39794 A (松下電器産業株式会社) 12. 2月.1999(12.02.99), 全頁を参照 (ファミリなし)	1-5, 8-10

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
11. 09. 01	25.09.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	中里 裕正	5M 9364
	電話番号 03－3581－1101 内線 3597	

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号 [redacted]T／JP01／05484

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2000-122539 A (松下電器産業株式会社) 28. 4月. 2000(28.04.00), 第18,44,45段落 (ファミリなし)	1-5,8-10
A	一松信 監修, データ保護と暗号化の研究 コンピュータ・ネットワークの安全性, 日本経済新聞社, 29.7月.1983(29.07.83), p.201-206 (特にp.204 3データ暗号鍵の登録 を参照)	1-5,8-10

10/069790

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)
1999P02699WO		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/DE00/02869	23/08/2000	30/08/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04M3/54		
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 4 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 5 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
08/03/2001	05.03.2002
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Kusztelan, L Tel. Nr. +49 89 2399 2479

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE00/02869

I. Grundlag des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

3-13	ursprüngliche Fassung			
1,2	eingegangen am	21/02/2002	mit Schreiben vom	21/02/2002

Patentansprüche, Nr.:

1-11	eingegangen am	21/02/2002	mit Schreiben vom	21/02/2002

Zeichnungen, Blätter:

1/4-4/4	ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   - ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
   - ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
   - ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequ nz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   - ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
   - ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
   - ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
   - ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
   - ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
   - ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:

   ☐ Ansprüche, Nr.:

   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-11
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-11
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-11
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
   siehe Beiblatt

Abschnitt V

Die in der unabhängigen Ansprüche 1 und 10 enthaltene Merkmalskombination ist aus dem vorliegenden Stand der Technik weder bekannt, noch wird sie durch ihn nahegelegt.

Durch die in den abhängigen Ansprüchen aufgeführten Maßnahmen sind vorteilhafte Weiterbildungen der in Anspruch 1 angegebene Vorrichtung dargestellt. Die Ansprüche erfüllen daher auch die in Art.33(1),(2) PCT genannten Kriterien.

Neue Beschreibungsseiten

Verfahren und System zum Umlenken von Fernmeldeverbindungen

Die vorliegende Erfindung betrifft ein Verfahren und ein System zum Umlenken von Fernmeldeverbindungen, das insbesondere die Einbindung von Teleworkern in ein Corporate Network ermöglicht.

Neben den üblichen Basisdiensten - in der Regel sind dies der Aufbau von Fernmeldeverbindungen und die Übertragung von Nutzdaten für die Kommunikation - werden von Anbietern öffentlicher Telekommunikationsnetze eine Reihe von ergänzenden Diensten angeboten. Die vorliegende Erfindung betrifft den Dienst der Rufumlenkung, der es einem Benutzer ermöglicht, ankommende Verbindungen unter verschiedenen Bedingungen auf andere Anschlüsse, beispielsweise zu automatischen Ansagen, zu einer Dienstperson (Operator) oder zu einem anderen Anschluß, unter dem der Benutzer vorübergehend erreichbar ist, umzulenken.

Eine derartige Rufumlenkung wird beispielsweise auch von sogenannten Teleworkern in Anspruch genommen. Darunter sind Mitarbeiter einer Firma zu verstehen, die zusätzlich zu ihrem Firmenarbeitsplatz zeitweise auch von zu Hause aus für die Firma arbeiten und insbesondere dort telefonisch erreichbar sein sollen. Bei einem derartigen Teleworker handelt es sich beispielsweise um einen Versicherungsagenten. Aktiviert dieser die Rufumlenkung, werden an seinem Firmenarbeitsplatz ankommende Telefonate automatisch zu seinem Heimanschluß umgelenkt.

Seit ungefähr 15 Jahren ist es möglich, beispielsweise bei ISDN-Verbindungen aber auch bei analogen Anschlüssen, die Rufnummer eines Gesprächspartners in Erfahrung zu bringen. Im Falle der ISDN-Verbindung werden dabei parallel zu den für die Kommunikation verwendeten Nutzdaten im B-Kanal Informationsdaten im D-Kanal übertragen, welche eine Anschlußkennung wiedergeben und von einem entsprechend ausgebildeten Fernmeldeapparat ausgewertet und angezeigt werden. Ruft daher der Teleworker im Rahmen seiner Berufstätigkeit von zu Hause aus einen Kunden an, so ist es für diesen ohne weiteres möglich, die Privatnummer des Teleworkers in Erfahrung zu bringen. Der Kunde wäre dann in der Lage, den Teleworker auch in solchen Zeiträumen zu Hause anzurufen, in denen dieser gar nicht arbeitet, und könnte diesen in seiner Freizeit stören. Ein weiteres Problem könnte beispielsweise auch dann entstehen, wenn der Teleworker den Arbeitsplatz wechselt und auf dem gleichen Gebiet für eine

neue Firma tätig ist. Für den Kunden, dem lediglich die Privatnummer des Teleworkers bekannt ist, wäre dieser Wechsel nicht ersichtlich, so daß dieser möglicherweise ebenfalls die Versicherung wechseln könnte. Ein derartiger Wechsel wäre aber von den Firmen selbst nicht erwünscht.

Es ist daher Aufgabe der vorliegenden Erfindung, ein Verfahren zum Umlenken von Fernmeldeverbindungen anzugeben, das ein hohes Maß an Flexibilität bietet und bei dem das Umlenken der Fernmeldeverbindungen für eine externe Person nicht ersichtlich ist.

Die Aufgabe wird durch ein Verfahren, das die Merkmale des Anspruchs 1 aufweist, gelöst.

Eine vorteilhafte Ausgestaltung der Erfindung ist in Anpruch 2 beschrieben. Dementsprechend wird bei dem erfindungsgemäßen Verfahren bei geschäftlichen Telefonaten grundsätzlich nur die Firmennummer angezeigt, nicht jedoch die Privatnummer. Aus Sicht des Kun-

Neue Patentansprüche

1. Verfahren zum Umlenken von Fernmeldeverbindungen, wobei eine an einen ersten Fernmeldeanschluß (A1, A5) gerichtete Fernmeldeverbindung automatisch zu einem zweiten Fernmeldeanschluß (A2) umgelenkt wird und mittels der Fernmeldeverbindung parallel zu Nutzdaten Informationsdaten übertragen werden, welche eine Anschlußkennung wiedergeben, dadurch gekennzeichnet, daß eine öffentliche Vermittlungsstelle (VST1) des ersten Fernmeldeanschlusses (A1, A5) und eine öffentliche Vermittlungsstelle (VST2) des zweiten Fernmeldeanschlusses (A1, A5) Mittel (L1) zum Speichern der Anschlußkennung des ersten Fernmeldeanschlusses (A1, A5), der Anschlußkennung des zweiten Fernmeldeanschlusses (A2) und einer Statusinformation, die besagt, ob die Umlenkung erfolgen soll, aufweisen,und daß die Umlenkung zu dem zweiten Fernmeldeanschluß (A2) an der öffentliche Vermittlungsstelle (VST1) des ersten Fernmeldeanschlusses (A1, A5) erfolgt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß in dem Status der Umlenkung der Fernmeldeverbindungen des ersten Fernmeldeanschlusses (A1, A5) zu dem zweiten Fernmeldeanschluß (A2) sowohl bei Aufbau einer Fernmeldeverbindung von dem zweiten Fernmeldeanschluß (A2) zu einem dritten Fernmeldeanschluß (A3) wie auch bei Aufbau einer Fernmeldeverbindung von einem dritten Fernmeldeanschluß (A3) zu dem zweiten Fernmeldeanschluß (A2) die mittels der Fernmeldeverbindung parallel zu den Nutzdaten übertragenen Informationsdaten so in den öffentlichen Vermittlungsstellen (VST1,VST2) modifiziert werden, daß sie anstelle der Anschlußkennung des zweiten Fernmeldeanschlusses (A2) die Anschlußkennung des ersten Fernmeldeanschlusses (A1, A5) wiedergeben.

3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß der erste Fernmeldeanschluß (A1) ein Anschluß innerhalb einer Nebenstellenanlage (PBX) ist.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die Nebenstellenanlage (PBX) Mittel zum Speichern der Anschlußkennung des ersten Fernmeldeanschlusses (A1) und einer Statusinformation, die besagt, ob eine Umlenkung erfolgen soll, aufweist,
und daß eine von einem vierten Fernmeldeanschluß (A4), der ebenfalls ein Anschluß innerhalb der Nebenstellenanlage

(PBX) ist, ausgehende und an den ersten Fernmeldeanschluß (A1) gerichteten Fernmeldeverbindung zu der öffentlichen Vermittlungsstelle (VST1) des ersten Fernmeldeanschlusses (A1) bzw. der Nebenstellenanlage (PBX) und von dort zu dem zweiten Fernmeldeanschluß (A2) umgelenkt wird.

5. Verfahren nach Anspruch 4,
dadurch gekennzeichnet,
daß bei der Eingabe einer nebenstellen-internen Anschlußkennung eine von dem zweiten Fernmeldeanschluß (A2) ausgehende Fernmeldeverbindung an die Nebenstellenanlage (PBX) und an den entsprechenden Nebenstellenanschluß (A4) geleitet wird.

6. Verfahren nach einem der vorherigen Ansprüche,
dadurch gekennzeichnet,
daß das Modifizieren der Informationsdaten durch Eingabe eines speziellen Steuersignals vorübergehend ausgeschaltet werden kann.

7. Verfahren nach einem der vorherigen Ansprüche,
dadurch gekennzeichnet,
daß dieses von dem zweiten Fernmeldeanschluß (A2) aus durch Eingabe eines vorgegebenen Zugangscode aktivierbar ist.

8. Verfahren nach einem der vorherigen Ansprüche,
dadurch gekennzeichnet,
daß der zu dem ersten Fernmeldeanschluß A1, A5) gehörende zweite Fernmeldeanschluß (A2) fest vorgegeben ist.

9. Verfahren nach einem der Ansprüche 1 bis 8,
dadurch gekennzeichnet,
daß der zu dem ersten Fernmeldeanschluß (A1, A5) gehörende zweite Fernmeldeanschluß (A2) beim Aktivieren des Umlenk-Verfahrens durch Übertragen eines Steuersignals frei gewählt werden kann.

10. System zum Umlenken von an einen ersten Fernmeldeanschluß (A1, A5) gerichteten Fernmeldeverbindungen zu einem zweiten Fernmeldeanschluß (A2), aufweisend:
eine mit dem ersten Fernmeldeanschluß (A1, A5) verbundene Vermittlungsstelle (VST1), die Mittel (L1) zum Speichern der Anschlußkennung des ersten Fernmeldeanschlusses (A1, A5), der Anschlußkennung des zweiten Fernmeldeanschlusses (A2), einer Statusinformation, die besagt, ob die Umlenkung erfolgen soll, sowie Mittel zum Umlenken von Fernmeldeverbindungen zu dem zweiten Anschluß (A2) aufweist;

eine mit dem zweiten Fernmeldeanschluß (A2) verbundene zweite Vermittlungsstelle (VST2), die Mittel (L2) zum Speichern der Anschlußkennung des ersten Fernmeldeanschlusses (A1, A5) und der Anschlußkennung des zweiten Fernmeldeanschlusses (A2), sowie Mittel zum Modifizieren von Informationsdaten, welche eine Anschlußkennung wiedergeben, aufweist.

11. System nach Anspruch 10,
dadurch gekennzeichnet,
daß es zusätzlich eine Nebenstellenanlage (PBX) enthält, wobei der erste Fernmeldeanschluß (A1) in diese Nebenstellenanlage (PBX) integriert ist, und die Nebenstellenanlage (PBX) Mittel zum Speichern einer Information, die besagt, ob an den ersten Fernmeldeanschluß (A1) gerichtete Fernmeldeverbindungen umgelenkt werden sollen, aufweist.